GALOIS THEORY

Emil Artin

目　　录

I. 线 性 代 数

II. 体　　论

III. 应　　用

A. N. Milgram

I

线 性 代 数

A. 体

体是一个集，对它的元定义了叫做加法和乘法的两种运算．这运算同实数系(它本身就是体的一个例子)里的加法和乘法相类似．在每个体 K 之中总有两个唯一确定了的叫做 0 和 1 的元，它们与 K 的另一些元相加或相乘的作用恰如实数系中相应的元所示．这种类似不足之处有二：1．并未假设每个体中的乘法都是可交换的；2．体还可能只由有限多个元所组成．

说得更确切些，体是一个集，它的元对于加法组成 Abel 群，而且不把零算在里面的元组成乘法群，还有这两个群的运算是用分配律来连系着的．容易看到，零与任意元之积仍为零．

一个体中的乘法如果是可交换的，就把它叫做**交换体**．如果要特地强调乘法非交换的这种可能性，那就称之为**斜体**．

B. 向量空间

设 V 是以 $A, B, \cdots$ 为元的 Abel 加法群，K 是以 $a, b, \cdots$ 为元的体．对于 K 的每个元 a 与 V 的每个元 A 还假设定义了积 aA 作为 V 的一元．如果下列的假设成立，集 V 就叫做 K 上的(左)**向量空间**：

1．$a(A+B)=aA+aB$,

2. $(a+b)A=aA+bA$,

3. $a(bA)=(ab)A$,

4. $1A=A$.

如果V是K上的向量空间，读者就容易证实，$oA=0$与$a0=0$成立，其中o与0分别是K与V中的零元．例如前一个关系式从下列方程推出：

$$aA=(a+o)A=aA+oA.$$

如果把积aA换成适合类似规律而定义的积Aa，V就叫做K上的右向量空间．如果左与右向量空间在讨论中不同时出现，就简称之为“向量空间”．

C．齐次线性方程

如果在体K中给定$n\cdot m$个元a_{ij}，$i=1, 2, \cdots, m$，$j=1, 2, \cdots, n$．要求下列方程组在K中的解x_i：

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & + \cdots + & a_{1n}x_n & = & 0, \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + \cdots + & a_{mn}x_n & = & 0. \end{array} \tag{1}$$

(1)叫做以$x_1, x_2, \cdots, x_n$为未知元的齐次线性方程组．如果（K中有满足这组方程的）元$x_1, x_2, \cdots, x_n$不都是o，就叫非平凡解，否则叫平凡解．

命题 1 线性齐次方程组有非平凡解，如果未知元的个数多于方程的个数．

证明所根据的方法是读者还在中学时就学过的，即用未知元的逐次消去法．如果$n(>0)$个变量的方程一个也没有（即$m=0$），那么未知元就不受任何限制，可把它们全部取作$=1$．

按完全归纳法来进行证明．假设未知元的个数多于 k 个而方程只有 k 个的那种方程组当 $k<m$ 时总有非平凡解．在方程组(1)中设 $n>m$ 而且把表式 $a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n$ 记作 L_i, $i=1, 2, \cdots, m$．我们来找那些不全为 o 的、使得 $L_1=L_2=\cdots=L_m=o$ 的 $x_1, x_2, \cdots, x_n$．如果对于每个 i 和 j 都有 $a_{ij}=o$，那么(在 K 中)任意选取的 $x_1, x_2, \cdots, x_n$ 就总是解．如果这些 a_{ij} 不全为 o，因为变更这些方程的次序或未知元的编码并不影响联立解的存在与否，所以可设 $a_{11}\neq 0$．要对给定的方程组能求得非平凡解，必须而且只须对于下列方程组能求得非平凡解：

$$
\begin{aligned}
&L_1=o\\
&L_2-a_{21}a_{11}^{-1}L_1=o\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&L_m-a_{m1}a_{11}^{-1}L_1=o.
\end{aligned}
$$

这是因为：如果 $x_1, x_2, \cdots, x_n$ 是刚才列出的方程组的解，由 $L_1=o$ 就使得其余所有方程中的第二项都消失，因此有 $L_2=L_3=\cdots=L_m=o$．反之，如果(1)成立，这组新的方程就显然成立．读者注意到新方程组是由后 $m-1$ 个方程“消去” x_1 而建立的．把后 $m-1$ 个方程当作 $x_2, \cdots, x_n$ 的方程组来看，如果它有非平凡解，那么取 $x_1=-a_{11}^{-1}(a_{12}x_2+a_{13}x_3+\cdots+a_{1n}x_n)$ 就得到整个方程组的解．然而按归纳假设，这后 $m-1$ 个方程是有非平凡解的，由此得到本命题．

注　方程组(1)中所有系数 a_{ij} 是 x_j 左方的因子．对于其中所有系数是右方因子的方程组，于是各个项换写成 x_ja_{ij}，用类似的证明使同样的命题成立．如果既有左方系数又有右方系数出现，那么在非交换的情形就作不出这样的命题．

D. 向量的相关性与无关性

体 K 上的向量空间 V 中向量 $A_1, A_2, \cdots, A_n$ 叫做**相关的**，如果 K 中有不全为 o 的元 $x_1, x_2, \cdots, x_n$ 存在，使得 $x_1A_1+x_2A_2+\cdots+x_nA_n=0$ 成立. 否则把向量 $A_1, A_2, \cdots, A_n$ 叫做**无关的**.

体 K 上的向量空间 V 的**维数**了解为 V 中无关向量的最大个数. 确切地说，向量空间的维数是无穷的，如果 V 中有任意多个无关的向量存在；如果 V 中有一组 n 个无关向量存在，而每组超过 n 个的向量总是相关的，V 就是 n 维的.

V 中一组元 $A_1, A_2, \cdots, A_m$ 叫做 V 的**生成系**，如果 V 的每个元 A 总能通过在 K 中适当地选取元 a_i, $i=1, \cdots, m$ 由 $A_1, A_2, \cdots, A_m$ 线性地表示出来，即

$$A=\sum_{i=1}^{m} a_iA_i.$$

命题 2 如果 V 有生成系 $A_1, A_2, \cdots, A_m$，那么这个生成系中无关向量的最大数就是 V 的维数.

证 如果所有的 $A_i=0$, V 就只由零向量组成. 如关系 $1\cdot 0=0$ 所示，零向量是相关的，因此 V 的维数为 o.

否则，设 r 为生成系 $A_1, A_2, \cdots, A_m$ 的无关向量最大数，通过重新编码就能实现 $A_1, A_2, \cdots, A_r$ 是无关的. 因为已设 r 是 A_i 中无关最大数，$r+1$ 个向量 $A_1, A_2, \cdots, A_r, A_i$ 就相关，因此有关系

$$a_1A_1+a_2A_2+\cdots+a_rA_r+b\cdot A_i=o,$$

其中系数不全为 0. 如果 $b=0$, $A_1, A_2, \cdots, A_r$ 就相关了. 因此 $b\neq 0$, 上式可写成

$$A_i=-b^{-1}(a_1A_1+a_2A_2+\cdots+a_rA_r).$$

从此得到，$A_1, A_2, \cdots, A_r$ 也是生成系；因为 V 中任一向量的线性表式中的 A_i 总可代以 $A_1, A_2, \cdots, A_r$ 的线性组合.

设 $B_1, B_2, \cdots, B_t$ 是 V 中某一组向量，$t>r$. 于是有 a_{ij} 使得 $B_j=\sum_{i=1}^{r} a_{ij}A_i$. 要证明这些向量 $B_1, B_2, \cdots, B_t$ 相关，就要证 K 中有不全为 0 的 x_i 存在，使得

$$x_1B_1+x_2B_2+\cdots+x_tB_t=0$$

成立. 在这方程中用 $\sum_{i=1}^{r} a_{ij}A_i$ 代 B_j，就得到 A_i 的一个线性组合，其中 $\sum_{j=1}^{t} x_ja_{ij}$ 为 A_i 的系数. 因此只须求得使方程组 $\sum_{j=1}^{t} x_ja_{ij}=0$, $i=1, 2, \cdots, r$ 成立的非平凡解 x_j. 由于 $t>r$ 和命题 1，这样的 x_j 是存在的.

既然个数比 r 多的向量组都相关，而向量 $A_1, A_2, \cdots, A_r$ 又无关，所以 r 就是 V 的维数.

注 n 维向量空间的任意 n 个无关向量 $A_1, A_2, \cdots, A_n$ 构成生成系. 因为任一向量 A 总与向量 $A_1, A_2, \cdots, A_n$ 相关，从而相关式中 A 的系数不能为零. 由 A 的解就证明了 $A_1, A_2, \cdots, A_n$ 构成生成系.

向量空间 V 的一个子集叫做**子空间**，如果它是这向量空间的子群而且这子集的任一元与体元相乘仍不出此子集. 如果 $A_1, A_2, \cdots, A_s$ 是向量空间 V 的元，所有形如 $a_1A_1+a_2A_2+\cdots+a_sA_s$ 的元就显然构成 V 的子空间. 由维数的定义得知，子空间的维数不超过全向量空间的维数.

设 V 是有限维 n 的向量空间，W 是具有同一维数 n 的 V 的子空间. 于是 $W=V$. 这子空间含有 n 个无关向量，它们其实构成 V 的生成系.

体 K 中 s 个元的序列 $(a_1, a_2, \cdots, a_s)$ 叫做**行向量**. 所

有这些 s 个元的序列由下列定义构成向量空间：

α) $(a_1, a_2, \cdots, a_s) = (b_1, b_2, \cdots, b_s)$ 当且仅当 $a_i = b_i$, $i=1, 2, \cdots, s$;

β) $(a_1, a_2, \cdots, a_s) + (b_1, b_2, \cdots, b_s) = (a_1+b_1, a_2+b_2, \cdots, a_s+b_s)$;

γ) $b(a_1, a_2, \cdots, a_s) = (ba_1, ba_2, \cdots, ba_s)$ 对于 K 中的元 b.

把 s 个元的序列写成纵列

$$\begin{pmatrix} a_1 \\ \vdots \\ a_s \end{pmatrix}$$

就叫做列向量.

命题 3 体 K 中所有 n 个元的序列构成的行(列)向量空间 K^n 是 K 上的 n 维向量空间.

证 n 个元(所谓单位向量)

$$\varepsilon_1 = (1, o, o, \cdots, o)$$
$$\varepsilon_2 = (o, 1, o, \cdots, o)$$
$$\vdots$$
$$\varepsilon_n = (o, o, o, \cdots, 1)$$

是无关的而且生成 K^n. 此二者都由关系

$$(a_1, a_2, \cdots, a_n) = \sum_{i=1}^{n} a_i \varepsilon_i$$

得以证明.

体 K 中的元作成的长方形阵列

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

叫做**矩阵**．矩阵的**右行秩**是指由体元右乘矩阵的行$(a_{i1}, a_{i2}, \cdots, a_{in})$时，各行之间得到的无关行向量的最大数．相应地定义左行秩，右列秩与左列秩．

命题 4 矩阵的右列秩等于左行秩，而且左列秩等于右行秩．如果体是可交换的，这四个数就相等，而且叫做矩阵的秩．

证 用$C_1, C_2, \cdots, C_n$来记矩阵的列向量，$R_1, R_2, \cdots, R_m$记其行向量．列向量0是

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

因此相关性$C_1x_1+C_2x_2+\cdots+C_nx_n=0$就等价于方程组

$$\begin{aligned} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n&=0, \\ \vdots \qquad\qquad\qquad & \vdots \\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n&=0 \end{aligned} \tag{1}$$

的解．矩阵中行的次序变更引出同一方程组，因此并不改变矩阵的列秩．行秩也不变，因为改变了的矩阵有同样的行向量．以s记矩阵的右列秩，z记左行秩．根据上述考虑可以假定矩阵的前z个行是无关的行向量．由矩阵中所有行生成的行向量的向量空间按命题2就有维数z，而且已由前z个向量生成．于是每一行可由前z个行线性地表出．因此(1)中前z个方程的任一解就是整个方程组的解；因为每个方程可作成前z个方程的线性组合．反之，(1)的每个解也是前z个方程的解．这就是说，由原来的矩阵中前z个行组成的矩阵

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{z1} & a_{z2} & \cdots & a_{zn} \end{pmatrix}$$

与原矩阵有相同的右列秩. 它们也有相同的左行秩, 因为这 z 个行是选为无关的. 然而由命题 3, 新矩阵的列秩不能超过 z. 因此 $s \leqslant z$. 仿此得到, 如以 s' 记左列秩, z' 记右行秩, 就有 $s' \leqslant z'$. 把原矩阵转置, 即行列互换, 于是转置矩阵的左行秩就等于原矩阵的左列秩. 上述讨论应用于转置矩阵就得到 $z \leqslant s$ 与 $z' \leqslant s'$.

E. 非齐次线性方程

现在来讨论非齐次线性方程组

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ \vdots \qquad\qquad\qquad \vdots \quad &\quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned} \tag{2}$$

的可解性问题. 有两个矩阵 M 与 N 与这组方程对应. M 为系数 a_{ij} 的矩阵; N 由 M 的第 i 行多加元 b_i 所组成. N 的列向量记作 $A_1, A_2, \cdots, A_n, B$. 组(2)能简写为式子:

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = B.$$

设 K^m 是所有 m 项列向量的右向量空间. K^m 中向量 $A_1, A_2, \cdots, A_n$ 生成 K^m 的一个子空间 T. 方程组的可解性得以简单地说明为 B 属于 T. T 的维数是矩阵 M 的右列秩. 因此方程的可解性就是说, M 与 N 有同样的右列秩. 所有这些只不过是对可解性的另一种说法而已. 引用命题 4 就看到, 方程(2)恰好在 M 和 N 有相同的左行秩时有解, 而且这

种说法在有的情况下可能有用.

如果 $m=n$, 方程个数就等于未知元个数, 这样还要考虑与(2)相连系的**伴随齐次方程组**

$$A_1x_1+A_2x_2+\cdots+A_nx_n=0.$$

下列问题的提法是最常见的:

给定系数 a_{ij} 的方程组(2)对于 K 中任意的 b_i 有解吗? 如果有, 就是说每个列向量 B 属于 T, 因此 T 就是整个空间 K^n. 既然 K^n 具有维数 n, 当这些向量 $A_1, A_2, \cdots, A_n$ 无关时, 正好就是如此. 而这就是说, 伴随齐次方程组只有平凡解. 而且每个向量 B 只能用一种方式表成向量 $A_1, A_2, \cdots, A_n$ 的线性组合. 于是就证明了

命题 5 如果方程组(2)中的 $m=n$, 那么对于方程右方是体中任意元的情形, 方程有解当且仅当伴随齐次方程组只有平凡解. 如果是这种情形, 那么这个解并且是唯一的.

F. 行 列 式

这儿所发挥的行列式论, 在 Galois 理论中并不需要. 因此, 读者可随意去留.

假设体是可交换的, 从而来考虑具有 n 行与 n 列的正方形矩阵

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}. \tag{1}$$

现在来定义这矩阵的某一函数, 它的值是体的元, 把这函数叫做行列式并记作

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} \tag{2}$$

或 $D(A_1, A_2, \cdots, A_n)$，如果把它看成(1)中列向量 $A_1, A_2, \cdots, A_n$ 的函数. 如果除 A_k 外的其它列都固定了，因而把行列式看成 A_k 的函数，就写成 $D_k(A_k)$，或者有时只写成 D.

定义 列向量的函数叫做行列式，如果它适合三条公理:

1. 作为任一列 A_k 的函数来看，它是线性的而且是齐次的，即

$$D_k(A_k+A'_k)=D_k(A_k)+D_k(A'_k), \tag{3}$$

$$D_k(cA_k)=c\cdot D_k(A_k). \tag{4}$$

2. 它的值$=0$，当两个相邻的列 A_k 与 A_{k+1} 相等时.

3. 它的值$=1$，如果每个 A_k 是单位向量 U_k,

$$U_1=\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\quad U_2=\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\quad \cdots,\quad U_n=\begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \tag{5}$$

一般来说，行列式是否存在这个问题暂先把它挂起来. 然而由公理得到一些推论:

a) 在(4)中取 $c=0$ 得到: 行列式为 0，如果它有一个列为 0.

b) $D_k(A_k)=D_k(A_k+cA_{k\pm1})$，或者: 行列式不变，如果把一个列的倍数加到与它相邻的列. 其实，根据公理 2 和方程(3)与(4)就得到

$$D_k(A_k+cA_{k\pm1})=D_k(A_k)+cD_k(A_{k\pm1})=D_k(A_k).$$

c) 考虑 A_k 与 A_{k+1} 这两列．这是能用 A_k 与 $A_{k+1}+A_k$ 来代替的．从前列减去后列就有新列 $-A_{k+1}$ 与 $A_{k+1}+A_k$. 把前列加到次列就得到 $-A_{k+1}$ 与 A_k. 最后把 -1 括出来．由此得出结论：行列式变号，如果将两相邻列互换．

d) 行列式等于零，如果其某两列相等．其实，在累次互换了充分的相邻列之后，任意两列可取成相邻的．至此就只需应用公理 2 了．

与 b)及 c)中相同的方法能证明下列较一般的规则：

e) 把一列的倍数加到另一列上，行列式之值不变．

f) 任意两列互换只变行列式的符号．

g) 设$(\nu_1, \nu_2, \cdots, \nu_n)$为下标$(1, 2, \cdots, n)$的一置换．把 $D(A_{\nu_1}, A_{\nu_2}, \cdots, A_{\nu_n})$中之列重排直到恢复原来的次序就得到

$$D(A_{\nu_1}, A_{\nu_2}, \cdots, A_{\nu_n}) = \pm D(A_1, A_2, \cdots, A_n).$$

其中 $\pm$ 为适当确定了的符号，它与 A_k 的特殊值是毫无关系的．代 A_k 以 U_k 就变成 $D(U_{\nu_1}, U_{\nu_2}, \cdots, U_{\nu_n}) = \pm 1$，从而这个符号就只与单位向量的置换有关[1]．

现在把每个向量 A_k 代以 $A_1, A_2, \cdots, A_n$ 的线性组合 A'_k 如下：

$$A'_k = b_{1k}A_1 + b_{2k}A_2 + \cdots + b_{nk}A_n. \tag{6}$$

在计算 $D(A'_1, A'_2, \cdots, A'_n)$ 时先把公理 1 应用于 A'_1，于是把这行列式分解成一个和；然后对每一项的 A'_2 应用同样的方法，等等，如此进行．结果得到

$$\begin{aligned} D(A'_1, A'_2, \cdots, A'_n) &= \sum_{\nu_1, \nu_2, \cdots, \nu_n} D(b_{\nu_1 1}A_{\nu_1}, b_{\nu_2 2}A_{\nu_2}, \cdots, b_{\nu_n n}A_{\nu_n}) \\ &= \sum_{\nu_1, \nu_2, \cdots \nu_n} b_{\nu_1 1}b_{\nu_2 2}, \cdots, b_{\nu_n n}D(A_{\nu_1}, A_{\nu_2}, \cdots, A_{\nu_n}), \end{aligned} \tag{7}$$

1) 按照它的推导，$\pm$ 号也与所选择的行列式无关．

其中这些 ν_i 彼此无关地取遍从 1 到 n 的值. 如果两个下标 ν_i 相等, 就有 $D(A_{\nu_1}, A_{\nu_2}, \cdots, A_{\nu_n})=0$; 所以只剩下那些项, 其中 $(\nu_1, \nu_2, \cdots, \nu_n)$ 是 $(1, 2, \cdots, n)$ 的置换. 故得

$$D(A_1', A_2', \cdots, A_n')$$
$$=D(A_1, A_2, \cdots, A_n)\cdot \sum_{(\nu_1, \cdots, \nu_n)} \pm b_{\nu_1 1}\cdot b_{\nu_2 2}\cdot\cdots\cdot b_{\nu_n n}, \qquad (8)$$

其中 $(\nu_1, \nu_2, \cdots, \nu_n)$ 取遍 $(1, 2, \cdots, n)$ 的全部置换; $\pm$ 表示与置换相连系的符号. 注意: 如果函数 D 只满足前两个公理, 那么总可以得到同样的公式(8).

从(8)可引出许多推论.

先假定公理 3 的有效性而把 A_k 特殊化为单位向量 U_k. 于是就有 $A_k'=B_k$, 其中 B_k 是矩阵 b_{ik} 的列向量. 方程(8)成为

$$D(B_1, B_2, \cdots, B_n)=\sum_{(\nu_1, \cdots, \nu_n)} \pm b_{\nu_1 1}\cdot b_{\nu_2 2}\cdot\cdots\cdot b_{\nu_n n}. \qquad (9)$$

这是对于行列式的一个显式, 它指出行列式由公理而唯一确定, 如果它一般存在的话. 采用公式(9), 公式(8)就可依下面的方式来写:

$$D(A_1', A_2', \cdots, A_n')$$
$$=D(A_1, A_2, \cdots, A_n)D(B_1, B_2, \cdots, B_n). \qquad (10)$$

这就是所谓行列式的乘法命题. (10)的左方就是以

$$c_{ik}=\sum_{\nu=1}^{n} a_{i\nu}b_{\nu k} \qquad (11)$$

为元的 n 阶正方形矩阵的行列式. c_{ik} 由 $D(A_1, A_2, \cdots, A_n)$ 的第 i 行元乘以 $D(B_1, B_2, \cdots, B_n)$ 的第 k 列相应的元、再把所得积连加.

现在把(8)中的 D 代以任一个满足第一与第二公理的函数 $F(A_1, A_2, \cdots, A_n)$, 与(9)相比较, 得

$$F(A_1', A_2', \cdots, A_n')$$
$$= F(A_1, A_2, \cdots, A_n) D(B_1, B_2, \cdots, B_n).$$

把 A_k 特殊地取为单位向量 U_k，就得到

$$F(B_1, B_2, \cdots, B_n) = c \cdot D(B_1, B_2, \cdots, B_n), \qquad (12)$$

其中 $$c = F(U_1, U_2, \cdots, U_n).$$

把(10)用下列方法来特殊化：如果 i 是在 1 与 $n-1$ 之间的一个确定的下标，对于 $k \neq i, i+1$，就取 $A_k = U_k$，$A_i = U_i + U_{i+1}$，$A_{i+1} = 0$. 这时就有 $D(A_1, A_2, \cdots, A_n) = 0$，因为有一列是 0. 因此也有 $D(A_1', A_2', \cdots, A_n') = 0$；而这行列式与以 b_{jk} 为元的行列式的差别只在其第 $i+1$ 行与第 i 行相等. 所以看到：

行列式等于零，如果相邻两行相等.

(9)中的每个被加项是一个乘积，其一个因子恰是一个确定的行，例如第 i 行的一个元. 这就证明了如果把行列式当作这一行的函数来考虑，它就是线性而且齐次的. 最后，对每一行选取相当的单位向量，就有行列式 = 1；因为这矩阵与把矩阵中的列都取为单位向量时相同. 因此，如果把行列式当作它的行向量的函数来考虑，它也满足三条公理. 根据已证过的行列式的唯一性就得到：

如果把行列式的行向量转置成列向量，也就是，如果把矩阵按主对角线作镜面反射，行列式不变.

行列式等于零，如果某两行相等. 它变号，如果两行互换. 它不变，如果把一行的倍数加到另一行.

现在来证明行列式的存在. 对于只有一行的矩阵 a_{11}，这个元 a_{11} 本身就是行列式. 假设 $n-1$ 阶行列式已经存在. 如果考虑 n 阶矩阵(1)，可把某些 $n-1$ 阶行列式同它连系如下：

设 a_{ik} 是(1)中一个特殊的元.在(1)中划掉第 i 行和第 k 列再来考虑留下的 $n-1$ 阶矩阵的行列式. 把这行列式乘以 $(-1)^{i+k}$, 叫做 a_{ik} 的代数余子式, 记作 A_{ik}. 符号 $(-1)^{i+k}$ 的分布按棋盘式排列,即

$$\begin{pmatrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}.$$

设 i 是 1 与 n 之间的某个数. 考虑矩阵(1)的下列函数 D:

$$D=a_{i1}A_{i1}+a_{i2}A_{i2}+\cdots+a_{in}A_{in}. \tag{13}$$

它是第 i 行及其代数余子式之积的和.

考虑 D 与给定的列, 例如 A_k 的相关性. 对于 $\nu\neq k$, $A_{i\nu}$ 与 A_k 线性相关,此时 $a_{i\nu}$ 与 A_k 无关. 对于 $\nu=k$,则 A_{ik} 与 A_k 无关而 a_{ik} 为此列之一元. 因此满足公理 1. 假设相邻两列 A_k 与 A_{k+1} 相等. 对于 $\nu\neq k, k+1$, 在 $A_{i\nu}$ 中有两个相等的列, 所以 $A_{i\nu}=0$. 用来计算 A_{ik} 与 $A_{i,k+1}$ 的行列式是相同的, 棋盘式排列的符号却相反; 因此 $A_{ik}=-A_{i,k+1}$, 而 $a_{ik}=a_{i,k+1}$. 于是 $D=0$, 从而公理 2 成立. 对于特殊情形 $A_\nu=U_\nu$ $(\nu=1, 2, \cdots, n)$, 当 $\nu\neq i$ 时 $a_{i\nu}=0$, 同时 $a_{ii}=1$ 及 $A_{ii}=1$. 得到 $D=1$, 因此公理 3 也成立. 由此既证明了 n 阶行列式的存在, 又证明了(13)这个所谓行列式按其第 i 行展开的公式成立. 公式(13)可推广如下: 在行列式中以第 j 行代第 i 行而按此新行展开. 对于$i\neq j$, 行列式为 0, 对于 $i=j$, 它就是 D:

$$a_{j1}A_{i1}+a_{j2}A_{i2}+\cdots+a_{jn}A_{in}=\begin{cases}D, 对于\ j=i,\\ 0,\ 对于\ j\neq i.\end{cases} \tag{14}$$

行列互换就得到公式

$$a_{1h}A_{1k}+a_{2h}A_{2k}+\cdots+a_{nh}A_{nk}=\begin{cases}D,\ 对于\ h=k,\\ 0,\ 对于\ h\neq k.\end{cases} \tag{15}$$

今设 A 为 n 行方阵而 B 为 m 行方阵，其行列式分别记为 $|A|$ 与 $|B|$. 再设 C 为 n 行与 m 列的矩阵. 作正方形的 $n+m$ 阶矩阵

$$\begin{pmatrix}A & C\\ 0 & B\end{pmatrix}. \tag{16}$$

其中 0 为 m 行 n 列的零矩阵. 如果把(16)这矩阵的行列式只看作 A 的列的函数，它显然满足前两个公理. 由(12)，其值为 $c\cdot|A|$，其中的 c 是在(16)中把 A 的列代以单位向量后所得行列式之值. 这个 c 还与 B 有关，而且把它看成 B 的行的函数时，显然满足前两个公理. 因此(16)的行列式等于 $d\cdot|A|\cdot|B|$，其中 d 是把 A 与 B 的列都代以单位向量这一特殊情形下的行列式. 把这个新行列式的后 m 列减去前 n 列的适当倍就可以 0 代 C. 由此得 $d=1$，于是得到公式

$$\begin{vmatrix}A & C\\ 0 & B\end{vmatrix}=|A|\cdot|B|. \tag{17}$$

仿此也可证明公式

$$\begin{vmatrix}A & 0\\ C & B\end{vmatrix}=|A|\cdot|B|. \tag{18}$$

公式(17)与(18)是 Lagrange 一个一般命题的特款，一般命题可由这些特款推导. 因为对于主要的应用有(17)与(18)已足够了，关于一般命题的叙述与论证，读者可参考论述行列式的任一读本.

现在来考究行列式为零的矩阵是怎样的．容易证明下列的一些事实：

a）如果 $A_1, A_2, \cdots, A_n$ 线性相关，那么 $D(A_1, A_2, \cdots, A_n)=0$．其实此时的某一列 A_k 就是其余那些列的线性组合．从列 A_k 减去这线性组合就成为 0，因此 $D=0$.

b）向量 $A_1, A_2, \cdots, A_n$ 如果线性无关，此时它们就是所有列作成的 K^n 空间的生成系，因此在方程(6)中可选择那些 b_{ik} 使得 $A'_k=U_k$．把 b_{ik} 的值应用到公式(8)中，(8)的左方就等于 1，所以必定 $D(A_1, A_2, \cdots, A_n)\neq 0$.

把这些结果合起来得到：

一个行列式等于零的充要条件是其列向量（或行向量）线性相关.

这结果的另一形式为：

n 个未知量的 n 个线性齐次方程组

$$a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n=0 \quad (i=1, 2, \cdots, n)$$

有非平凡解的充要条件是其系数行列式为零.

显然也证明了：

线性方程组

$$a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n=b_i \quad (i=1, 2, \cdots, n) \tag{19}$$

对于任意的 b_i 值有解的充要条件是 a_{ik} 的行列式不等于 0.

最后，对于 a_{ik} 的行列式不为 0 的情形，用行列式来表出(19)的解.

方程(19)就是

$$A_1x_1+A_2x_2+\cdots+A_nx_n=B.$$

用 B 来代 $D(A_1, A_2, \cdots, A_n)$ 中的第 i 列，就是指的 $D(A_1, \cdots, B, \cdots, A_n)$．从 B 这一列减去 $A_\nu(\nu\neq i)$ 的倍数就剩了 A_ix_i．因此有

$$D(A_1, \cdots, B, \cdots, A_n) = x_i D(A_1, A_2, \cdots, A_n),$$

从而得到

$$x_i = \frac{D(A_1, \cdots, B, \cdots, A_n)}{D(A_1, A_2, \cdots, A_n)}.$$

这个公式以 Cramer 法则闻名.

II

体　论

A. 扩　体

所考虑的体都假设为交换体. 设 E 为体, K 是 E 的子集, 如果 K 对于 E 中所定义的加与乘自成一体, 即 K 是 E 的子体, 就称 E 为 K 的**扩张**. E 是 K 的扩张这关系简写成 $K \subset E$. 设 $\alpha, \beta, \gamma, \cdots$ 是 E 的一些元, 把 $K(\alpha, \beta, \gamma, \cdots)$ 了解为 E 中那些可以表成用 K 中元为系数的 $\alpha, \beta, \gamma, \cdots$ 的多项式的商的集. 显然 $K(\alpha, \beta, \gamma, \cdots)$ 是包含 $\alpha, \beta, \gamma, \cdots$ 这些元的、K 的最小扩张. 称为由 K 通过添加这些元 $\alpha, \beta, \gamma, \cdots$ 而得到的或**生成的体**.

设 $K \subset E$, E 就可以当作 K 上的向量空间来看, 因为这时把向量空间所需运算同化为 E 中所定义的运算. E 在 K 上的**次数**记作 (E/K), 了解为 K 上的向量空间 E 的维数. 对于有限的 (E/K), 称 E 为**有限的体扩张**.

命题 6　设 K, B, E 是三个体, 如果有关系 $K \subset B \subset E$, 那么

$$(E/K) = (E/B)(B/K).$$

证　设 E 的一组元 $A_1, A_2, \cdots, A_r$ 在 B 上线性无关, B 的一组元 $C_1, C_2, \cdots, C_s$ 在 K 上线性无关. 此时具有 $i=1, 2, \cdots, s$ 与 $j=1, 2, \cdots, r$ 的积 C_iA_j 是 E 的一组在 K 上线性无关的元. 这是因为, 如果 $\sum\limits_{i,j} a_{ij}C_iA_j = 0$, 就有 $\sum\limits_{j}\left(\sum\limits_{i} a_{ij}C_i\right)A_j$

$=0$，左方是以 B 中元为系数的 A_j 的线性组合，并且因为相对于 B 这些 A_j 是无关的，所以 $\sum_i a_{ij}C_i=0$ 对每个 j 成立．相对于 K 这些 C_i 的线性无关性就推导出全部的 $a_{ij}=0$．既然有 $r\cdot s$ 个元 C_iA_j，对每个 $r\leqslant(E/B)$ 与 $s\leqslant(B/K)$ 已证明了 $(E/K)\geqslant r\cdot s$，所以 $(E/K)\geqslant(B/K)(E/B)$．如果这后两个数有一个无穷，那么命题就证明了．如果两个数 (E/B) 与 (B/K) 都有限，取为 r 与 s 就能假设那些 A_j 与 C_i 分别是向量空间 E 与 B 的生成系．要证这些积 C_iA_j 组成在 K 上的 E 的生成系．E 中每个 A 可用 B 中元作系数通过这些 A_j 来线性表示．因此 $A=\sum B_jA_j$．每个 B_j 可以用 K 中元作系数通过这些 C_i 来线性表示，即 $B_j=\sum_i a_{ij}C_i$，$j=1, 2, \cdots, r$．于是 $A=\sum a_{ij}C_iA_j$，这些 C_iA_j 就构成 K 上的 E 的生成系。

系　如果

$$K\subset K_1\subset K_2\subset\cdots\subset K_n,$$

就有

$$(K_n/K)=(K_1/K)\cdot(K_2/K_1)\cdot\cdots\cdot(K_n/K_{n-1}).$$

B．多　项　式

形如 $a_0x^n+a_1x^{n-1}+\cdots+a_n$ 的表式中，如果 $a_0, \cdots, a_n$ 这些系数都是 K 的元并且 $a_0\neq0$，这表式就称为 K 中的**多项式**．其乘法与加法依常例[1]．

K 中的一个多项式如果能写成 K 中两个正次多项式之积，这多项式就称为在 K 中**可约**．在 K 中不是可约的非常数多项式称为在 K 中**不可约的**．

1）提到次数 $<n$ 的所有多项式的集也把多项式 0 算进去，虽然它在通常意义下是没有次数的。

$f(x)$，$g(x)$与$h(x)$这些K中的多项式如果满足方程$f(x)=g(x)\cdot h(x)$，就说$g(x)$整除$f(x)$或$g(x)$是$f(x)$的因子．容易看到$f(x)$的次数是$g(x)$的次数与$h(x)$的次数之和．如果$g(x)$与$h(x)$都不是常量，那么二者的次数都低于$f(x)$的次数．由此得到，多项式总可表成K中有限个不可约多项式之积．

对任意两个多项式$f(x)$与$g(x)$，有除法算式，即$f(x)=q(x)\cdot g(x)+r(x)$，其中$q(x)$与$r(x)$是K中唯一决定的多项式，而且$r(x)$的次数小于$g(x)$的次数．这是可以用初等代数中对于实数体或复数体的情形相同的方法来证明的．还看到$r(x)$是次数小于$g(x)$的唯一的多项式，使得$f(x)-r(x)$可被$g(x)$所整除．$r(x)$称为模$g(x)$的$f(x)$的余式．

用常法还可证明，$x-\alpha$为$f(x)$的因子，当且仅当α为$f(x)$的根．由此容易得出，体中多项式在体中所有的根的个数不能超过此多项式的次数．

引理　如果$f(x)$是K中的n次不可约多项式，那么K中不能有两个这样的非零多项式，其次数都小于n而其积被$f(x)$所整除．

否则，就有两个这样的多项式$g(x)$与$h(x)$，其次数都小于n，其积可被$f(x)$整除．对于所有可能的这样的多项式$g(x)$与$h(x)$，就选择$g(x)$是其中次数最小的．因为$f(x)$是$g(x)\cdot h(x)$的因子，就有多项式$k(x)$使得

$$k(x)\cdot f(x)=g(x)\cdot h(x).$$

根据除法算式有

$$f(x)=q(x)\cdot g(x)+r(x),$$

其中$r(x)$的次数小于$g(x)$的次数．$f(x)$既是不可约的，必定$r(x)\neq 0$．以$h(x)$乘此式并且通过适当的变形得到

$$r(x)\cdot h(x)=f(x)\cdot h(x)-q(x)\cdot g(x)\cdot h(x)$$
$$=f(x)\cdot h(x)-q(x)\cdot k(x)\cdot f(x),$$
由此得出 $r(x)\cdot h(x)$可被 $f(x)$整除. 但是这与 $g(x)$的选择相矛盾,因为 $r(x)$的次数是小于 $g(x)$的次数的. 因此证明了引理.

已看到初等代数的许多命题在任意的体 K 中也是成立的. 然而著名的代数基本定理则至少在其通常形式下不起作用. 它被 Kronecker 奠定的一个命题所取代,保证对于 K 中给定的多项式有一扩体存在, 这多项式在这扩体中有根. 此外, 还将证明, 在给定的体中, 多项式不仅可分解成不可约因子, 而且除了常因子外此种分解是唯一的. 唯一性和 Kronecker 的这个命题有关.

C. 代 数 元

设 K 为体,E 是 K 的一个扩体,于是, 如果 α 是 E 之一元, 那么试问, 在 K 中是否有以 α 为根的多项式存在. 如果有这样的非零多项式, α 就称为 **K 上的代数元**. 今设 α 是代数的. K 中以 α 为根的所有多项式中选出一个具最小次数的并且乘以 K 中适当的常量, 把这样得到的多项式记作 $f(x)$, 它的最高系数是 1.

现在来证 $f(x)$这多项式具有三个性质:

1. 如果 $g(x)$是 K 中多项式适合 $g(\alpha)=0$, 那么 $g(x)$可被 $f(x)$整除,

2. $f(x)$是不可约的,

3. $f(x)$由它的作法所用性质而唯一决定.

其实, 如果 $g(x)$是 K 中多项式具有 $g(\alpha)=0$, 就可写成 $g(x)=f(x)q(x)+r(x)$, 其中 $r(x)$的次数小于 $f(x)$的次数.

通过$x=\alpha$的代入得到$r(\alpha)=0$. 因为$r(x)$有α为根而其次数又小于$f(x)$, $r(x)$就一定是零多项式. 因此$g(x)$可被$f(x)$整除, 由此证明了性质1. 同时也就证明了如3所述的唯一性. 如果还设$f(x)$在K中是可以分解的, 那么对于$x=\alpha$, 必有一因子消失, 这就又与$f(x)$的选择矛盾. 因此也证明了2这性质.

现在来考虑E中由下列元θ组成的子集E_0:

$$\theta=g(\alpha)=c_0+c_1\alpha+c_2\alpha^2+\cdots+c_{n-1}\alpha^{n-1}.$$

这里$g(x)$是K中的次数小于n(n是$f(x)$的次数)的多项式. E_0这集对于加法与乘法都是封闭的. 后者证明如下:

设$g(x)$与$h(x)$是两个次数小于n的多项式. 取$g(x)h(x)=q(x)f(x)+r(x)$, 就得到$g(\alpha)h(\alpha)=r(\alpha)$. 最后看到$c_0$, c_1, $\cdots$, c_{n-1}这些常量由θ这个元唯一决定. 事实上, 若同一个θ有两个表式, 相减就引出一个次数小于n的α的方程.

注意, 集E_0的内部结构并不依赖于α的构造性质, 而只与这个不可约的$f(x)$有关. 这个多项式使得在E_0中可以实行加与乘. 即将看到E_0是体; 实际上就是$K(\alpha)$这个体. 如果这得到证明, 也就决定了次数$(K(\alpha)/K)$. 它必定等于n, 因为空间$K(\alpha)$由线性无关的元1, α, α^2, $\cdots$, α^{n-1}生成.

现在不用扩体E与元α. 仿照E_0那样来作. 仅只假定给出了不可约多项式

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0.$$

选一个符号ξ. 并设E_1是次数小于n的所有形式多项式

$$g(\xi)=c_0+c_1\xi+\cdots+c_{n-1}\xi^{n-1}$$

的集. 此集构成加法群. 现在随着通常的乘法来导出E_1中两个多项式$g(\xi)$与$h(\xi)$的新式乘法, 并且把它记作$g(\xi)$

$\times h(\xi)$．如此表示的积定义为通常的积 $g(\xi)h(\xi)$ 模 $f(\xi)$ 的余式 $r(\xi)$．首先注意到任意 m 个因子 $g_1(\xi), g_2(\xi), \cdots, g_m(\xi)$ 之积仍为常积 $g_1(\xi)g_2(\xi)\cdots g_m(\xi)$ 的余式．因为对于 $m=2$，由定义，这是对的，由下列易于证明的引理，按 m 作归纳法就得以证明．

引理 设 $r_1(\xi)$ 与 $r_2(\xi)$ 分别是两个多项式 $g_1(\xi)$ 与 $g_2(\xi)$ 的余式，那么积 $g_1(\xi)g_2(\xi)$ 与 $r_1(\xi)r_2(\xi)$ 就有相同的余式．

读者自证．这事实指出，新积是可结合的与可交换的，而且还得到，如果通常的积 $g_1(\xi)g_2(\xi)\cdots g_m(\xi)$ 的次数小于 n，那么新积 $g_1(\xi)\times g_2(\xi)\times\cdots\times g_m(\xi)$ 与通常的积就是一致的．新的乘法的分配律同样容易证明．

集 E_1 包含体 K，而且在 E_1 中的新乘法对于 K 就有原来的乘法意义．ξ 是 E_1 的一个多项式．把它自乘 i 次，显然只当 $i<n$ 时才得到 ξ^i．对于 $i=n$，就应当算出多项式 ξ^n 的余式．它就是

$$\xi^n-f(x)=-a_{n-1}\xi^{n-1}-a_{n-2}\xi^{n-2}-\cdots-a_0.$$

现在保持新的乘法，把老的乘法一起放弃，同时用点(或挨着写)来代替新乘法的记法．

在这种意义下来计算

$$c_0+c_1\xi+c_2\xi^2+\cdots+c_{n-1}\xi^{n-1},$$

容易得到仍是这个元，因为它所含项的次数都是低于 n 的．但是

$$\xi^n=-a_{n-1}\xi^{n-1}-a_{n-2}\xi^{n-2}-\cdots-a_0,$$

因此 $f(\xi)=0$．

于是就作出了集 E_1 和 E_1 中的加法与乘法，集 E_1 满足了体公理的大部分．E_1 把 K 作为子体，而 ξ 适合方程 $f(\xi)=0$．其次就应当证明：如果 $g(\xi)\neq 0$ 而且 $h(\xi)$ 是 E_1 中

给定的元，那么 E_1 中还有一元

$$X(\xi)=x_0+x_1\xi+\cdots+x_{n-1}\xi^{n-1}$$

存在，使得

$$g(\xi)\cdot X(\xi)=h(\xi).$$

为了证明这个，把 $X(\xi)$ 的系数看成未知量并算出左方的积，其中用 $f(\xi)=0$ 来简约 ξ 的那些较 $n-1$ 次为高的幂. 于是得出表式 $L_0+L_1\xi+\cdots+L_{n-1}\xi^{n-1}$，其中每个 L_i 都是以 K 中元为系数的 x_i 的线性组合. 因为这个表式等于 $h(\xi)$，由此得到 n 个未知量的 n 个方程

$$L_0=b_0,\ L_1=b_1,\ \cdots,\ L_{n-1}=b_{n-1},$$

其中 b_i 是 $h(\xi)$ 的系数. 如果相应的齐次方程

$$L_0=0,\ L_1=0,\ \cdots,\ L_{n-1}=0$$

只有平凡解，上组方程就是可解的.

如果要求满足 $g(\xi)\cdot X(\xi)=0$ 的 $X(\xi)$，这些齐次方程就出现了. 用旧的乘法来看，这就是说，通常的积 $g(\xi)X(\xi)$ 有余式 0，所以这积可被 $f(x)$ 整除. 由 B 段证明的引理，只有 $X(\xi)=0$ 才是可能的.

所以 E_1 是体.

此外，还假设有原来的扩张 E，其中有 $f(x)$ 的根 α，因此又有与它联系的集 E_0. 如果把 E_1 的元 $g(\xi)$ 映成 E_0 的 $g(\alpha)$，E_0 在一定的意义下有与 E_1 相同的结构. 这映射的性质是，元素和的象是单个元的象的和，积的象是各个元的象的积.

由这映射引出了把体 K 映到另一体 K' 的更为普遍的映射 σ，这样，对应于 K 中每个元 a，有 K' 中一个象元 $\sigma(a)$. 映射具有下列性质：

1. $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$,
2. $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$

对于 K 中所有元 α, β 都成立.

如果有一个 $\alpha\neq 0$ 使得 $\sigma(\alpha)=0$, 那么由 2, 对于每个 β 就有

$$\sigma(\beta)=\sigma(\alpha\cdot\alpha^{-1}\beta)=\sigma(\alpha)\cdot\sigma(\alpha^{-1}\beta)=0\cdot\sigma(\alpha^{-1}\beta)=0,$$

因此看到把整个的 K 映成 0. 当然这种映射毫无兴趣, 就还要求

3. 由 $\alpha\neq 0$ 得到 $\sigma(\alpha)\neq 0$.

如果在 1. 中取 $\alpha=0$, 就得到 $\sigma(\beta)=\sigma(0)+\sigma(\beta)$, 从而 $\sigma(0)=0$. 如果在 1. 中以 $-\alpha$ 代 β 就得到 $0=\sigma(\alpha)+\sigma(-\alpha)$ 或 $\sigma(-\alpha)=-\sigma(\alpha)$, 因此也有规律 $\sigma(\alpha-\beta)=\sigma(\alpha)-\sigma(\beta)$. 如果在 2. 中取 $\alpha=\beta=1$, 注意到 3. $\sigma(1)\neq 0$, 所以 $\sigma(1)=1$. 如果取 $\beta=\alpha^{-1}$, 由 2. 得 $\sigma(\alpha^{-1})=(\sigma(\alpha))^{-1}$, 由此得到法则 $\sigma\left(\frac{\alpha}{\beta}\right)=\frac{\sigma(\alpha)}{\sigma(\beta)}$. 最后, 由 $\sigma(\alpha)=\sigma(\beta)$ 得到 $\sigma(\alpha-\beta)=0$, 3. 又指出必定 $\alpha=\beta$. 所以 σ 是映 K 到 K' 的一一映射, 它保持所有运算, 这样的映射记为从 K 到 K' 的**同构**. 其象集是 K' 的子体.

如果这映射 σ 把 K 映成 K', 它就称为映 K 成 K' 的同构. 设 σ 是映 K 成 K' 的同构, 也就可以考虑把 K' 回转成 K 的逆映射 σ^{-1}, 不难看到这是映 K' 成 K 的同构. 如果存在一个映 K 成 K' 的同构, 就说 K 与 K' 是同构的.

定义并不排斥 K' 与 K 是同一个体. 如果 σ 是映 K 成自身的同构映射, 就把 σ 称为 K 的**自同构**. 此时 σ^{-1} 也是 K 的自同构. 例如把 K 映成自身的恒同映射就是 K 的自同构.

由这些定义得到, 集 E_0 也是体, E_0 与 E_1 同构.

设 σ 是映 K 成 K' 的同构, 把 K 中元 a 的象 $\sigma(a)$ 简记

作 a'. 把 σ 开拓到 K 的多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 上就是把 $f(x)$ 的象 $f'(x)$ 定义成

$$f'(x)=a_0'+a_1'x+\cdots+a_n'x^n.$$

容易看到下列两个方程是成立的:

$$(f(x)+g(x))'=f'(x)+g'(x),$$

$$(f(x)g(x))'=f'(x)g'(x).$$

不难看出, K 中不可约多项式 $f(x)$ 的象 $f'(x)$ 是 K' 中的不可约多项式.

现在作出一些命题,都由前所论证得出.

命题 7(Kronecker) 如果 $f(x)$ 是体 K 中的非常量多项式,那么有 K 的扩张 E 存在,使得其中有 $f(x)$ 之一根.

证 作出扩体,使得其中有 $f(x)$ 的一个不可约因子之一根.

命题 8 设 σ 是映体 K 成体 K' 的同构映射,再设 $f(x)$ 是 K 中不可约多项式而且 $f'(x)$ 是 K' 中相应的象多项式. 如果 $E=K(\beta)$ 与 $E'=K'(\beta')$ 分别是 K 与 K' 的扩张, E 中 $f(\beta)=0$, E' 中 $f'(\beta')=0$, 那么 σ 可开拓为 E 与 E' 之间的同构,其中 β' 是 β 的象.

证 E 的每个元 θ 具形式 $\theta=g(\beta)$, 其中 $g(x)$ 是 K 中的次数小于 $f(x)$ 的次数的多项式. 把 $\theta'=g'(\beta')$ 作为 θ 的象. 显然这个映射就是给定的映射 σ 的开拓, 而且把 E 映成 E'. 它把两个元的和映成象元的和是明显的. 积也是适合相应的法则的,因为 $g(\beta)h(\beta)=r(\beta)$ 的意义是, $r(x)$ 为 $g(x)h(x)$ 模 $f(x)$ 的余式. 因此有多项式 $q(x)$ 使得 $g(x)h(x)=q(x)f(x)+r(x)$. 把它换成象就得到 $g'(x)h'(x)=q'(x)f'(x)+r'(x)$, 所以 $x=\beta$ 就有 $g'(\beta')h'(\beta')=r'(\beta')$.

命题 8 非常明白地指出: 由不可约方程之一根所生成的

扩体，其结构与此根的特性无关.

D. 分 裂 体

如果 K，B 与 E 是这样的三个体：$K\subset B\subset E$，就把 B 称为**中间体**.

设 $p(x)$ 为 K 中多项式，E 为 K 的扩张，$p(x)$ 在其中可分解成线性因子. 显然如此的线性分解总可以写成

$$p(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)$$

的形式. 此时 a 显为 $p(x)$ 的最高次系数，即为属于 K 的元.

E 的子体，其中可能有此分解者显然含有 $p(x)$ 的这些根 $\alpha_1, \alpha_2, \cdots, \alpha_s$. 由此得到，其中可能如此分解的最小中间体就是 $K(\alpha_1, \alpha_2, \cdots, \alpha_s)$ 这个体. 此体称为在 K 上 $p(x)$ 的**分裂体**，或在不致误解的时候干脆称为 $p(x)$ 的分裂体.

分裂体之存在由下述论证落实. 根据命题 7 先把 K 作如此的扩张，使得分解 $p(x)=(x-\alpha_1)p_1(x)$ 是可能的. 重复引用此法于 $p_1(x)$，直到最后得到其中 $p(x)$ 分解成线性因子的 K 的扩体为止. 于是得出

命题 9 如果 $p(x)$ 为体 K 中的多项式，那么就有 $p(x)$ 的分裂体 E 存在.

对分裂体 $E=K(\alpha_1, \alpha_2, \cdots, \alpha_s)$ 可得递升的体链：$K=E_0\subset E_1\subset\cdots\subset E_s=E$，其中 $E_i=K(\alpha_1, \alpha_2, \cdots, \alpha_i)=E_{i-1}(\alpha_i)$. 因为 $p(\alpha_i)=0$ 并且 $p(x)$ 自然也是 E_{i-1} 中的多项式，α_i 就是 E_{i-1} 上的代数元. 所以次数 (E_i/E_{i-1}) 为有限，从而 $p(x)$ 的分裂体的次数 (E/K) 也是有限的.

另一方面，下列命题指出多项式的分裂体在同构的意义上是唯一决定的.

命题 10 设 σ 为映体 K 成体 K' 的同构，$p(x)$ 是 K 中

的多项式，它在 K' 中的象为 $p'(x)$，E 为 $p(x)$ 的分裂体，E' 为 $p'(x)$ 的分裂体. 那么 σ 就可开拓为 E 与 E' 间的同构.

证 设 $p(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)$ 为 $p(x)$ 在 E 中的分解. 如果所有的 α_i 都属于 K，就有 $E=K$，因此把 σ 直接作用于此分解得到 $p'(x)$ 在 K' 中的分解. 于是 $E'=K'$，从而命题在这种情况得证.

现在对不在 K 中的 n 个 α_i 来作归纳法. 因此可设 $n>1$，而且假设命题对不在 K 中的根的个数小于 n 者已证明了. 设 α_1 不在 K 中，以 α_1 为其根的 K 中不可约多项式设为 $f(x)$. 既然 $p(\alpha_1)=0$，就有分解式 $p(x)=f(x)g(x)$，由此得 $p'(x)=f'(x)g'(x)$. 设 $p'(x)=a'(x-\beta_1)(x-\beta_2)\cdots(x-\beta_s)$ 为 E' 中 $p'(x)$ 的分解式. $f'(x)$ 在 E' 的扩体中有根 γ，从而 $p'(\gamma)=0$; 因此 $a'(\gamma-\beta_1)(\gamma-\beta_2)\cdots(\gamma-\beta_s)=0$. 由此得 β_i 之一（设为 β_1）就是 $f(x)$ 的根 γ. 根据命题 8，同构 σ 可开拓为映 $K(\alpha_1)$ 成 $K'(\beta_1)$ 的同构 τ. 把 $p(x)$ 当作 $K(\alpha_1)$ 中之多项式，$p'(x)$（$p(x)$ 的 τ 象）看成 $K'(\beta_1)$ 中的多项式. E 就是 $p(x)$ 在 $K(\alpha_1)$ 上的分裂体，而且 E' 就是 $p'(x)$ 在 $K'(\beta_1)$ 上的分裂体. $p(x)$ 在 $K(\alpha_1)$ 中的根的个数至少比 $p(x)$ 在 K 中的根数多一个. 于是不在 $K(\alpha_1)$ 中的根的个数就小于 n. 由归纳假设 τ 就可开拓为映 E 成 E' 的同构，它显然也是 σ 的开拓.

系 如果 $p(x)$ 是体 K 中的多项式，那么 $p(x)$ 的两个任意的分裂体相互同构.

取 $K'=K$ 并且把 σ 取为恒同映射，即 $\sigma(x)=x$，由命题 10 得到本系.

根据本系，简用“$p(x)$ 的分裂体”这个述语就是正当的，因为 $p(x)$ 的两个任意的分裂体同构. 如果 $p(x)$ 在其一个分裂

体内有重根，那么在其另一分裂体中亦然．“$p(x)$有重根”这个述语因此与分裂体无关．

读者在考虑 K 为有理数体这种特款时就会明了刚才所证唯一性命题的意义．如果 $p(x)$ 为此体中之不可约多项式，从而求得一个扩体 $K(\alpha)$ 使得 $p(\alpha)=0$，那么对这种体的作法有二．第一法如C节中所述的抽象方法，第二法根据所谓代数学的基本定理，由此可求得复数 α' 适合 $p(\alpha')=0$．第二法与第一法显著不同，因为 α' 的作法引用到极限和分析的其它方法．但是，根据命题8可知 $K(\alpha)$ 与 $K(\alpha')$ 这两个体是同构的．由命题10，对多项式的分裂体有相似的命题．因此，对于代数命题的论证用不着这个代数学的基本定理．

E．多项式分解成不可约因子的唯一可分解性

命题11　如果 $p(x)$ 是体 K 中的多项式，而且

$$p(x)=p_1(x)\cdot p_2(x)\cdot\cdots\cdot p_r(x)=q_1(x)\cdot q_2(x)\cdot\cdots\cdot q_s(x)$$

是 $p(x)$ 分解成 K 中不可约多项式的两种因子分解式，其中每个因子至少是一次多项式，那么 $r=s$，而且由 q_i 的适当编号得到 $p_i(x)=c_iq_i(x)$，其中的 c_i，$i=1, 2, \cdots, r$ 都是 K 中的元．

证　取 K 的扩张，使得其中有 $p_1(x)$ 之一根 α．把 $x=\alpha$ 代入 $p_1(x)p_2(x)\cdots p_r(x)=q_1(x)q_2(x)\cdots q_s(x)$，就有

$$0=q_1(\alpha)q_2(\alpha)\cdots q_s(\alpha),$$

因此必定有一因子，设为 $q_1(\alpha)$，是零．所以 $q_1(x)$ 可被 $p_1(x)$ 整除，因为 $q_1(x)$ 不可约，故得 $p_1(x)=c_1q_1(x)$，其中的 c_1 属于 K．将此代入分解式再约去因子 $q_1(x)$，就得到 $c_1p_2(x)\cdots p_r(x)=q_2(x)\cdots q_s(x)$．由归纳法得到命题的证明．

F. 群特征标

设 G 为乘法群, K 为体. σ 是映 G 到 K 的这样的映射: 对 G 中所有的 α, β 有 $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$. 如果有一个 α 使得 $\sigma(\alpha)=0$, 那么对 G 中任一个 β 就有

$$\sigma(\beta)=\sigma(\alpha\cdot\alpha^{-1}\beta)=\sigma(\alpha)\sigma(\alpha^{-1}\beta)=0.$$

这种 σ 不重要. 因此还要求对 G 中所有的 α 都有 $\sigma(\alpha)\neq 0$. 把这样的映射 σ 称为从 G 到 K 的**特征标**.

命题 12 设 G 为乘法群, $\sigma_1, \sigma_2, \cdots, \sigma_n$ 为两两不同的从 G 到体 K 的特征标. 那么 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 是线性无关的; 就是说, 如果 K 中有元 $a_1, a_2, \cdots, a_n$ 使得方程 $a_1\sigma_1(x)+a_2\sigma_2(x)+\cdots+a_n\sigma_n(x)=0$ 对 G 中所有的 x 都成立, 那么 $a_1=a_2=\cdots=a_n=0$.

证明用归纳法. 对 $n=1$, 由 $a_1\sigma_1(x)=0$ 得到 $a_1=0$, 因为 $\sigma_1(x)\neq 0$. 设 $n>1$, 假定此命题对小于 n 个特征标的已证明. 把一个假设的关系用如下两种方法来变形.

设 α 是 G 中的待定的元. 第一变形是以 αx 代 x, 第二是以 $\sigma_n(\alpha)$ 乘原来的关系. 这样得到的两个关系是

$$a_1\sigma_1(\alpha)\sigma_1(x)+a_2\sigma_2(\alpha)\sigma_2(x)+\cdots+a_n\sigma_n(\alpha)\sigma_n(x)=0,$$
$$a_1\sigma_n(\alpha)\sigma_1(x)+a_2\sigma_n(\alpha)\sigma_2(x)+\cdots+a_n\sigma_n(\alpha)\sigma_n(x)=0.$$

相减得

$$a_1(\sigma_1(\alpha)-\sigma_n(\alpha))\sigma_1(x)+\cdots$$
$$+a_{n-1}(\sigma_{n-1}(\alpha)-\sigma_n(\alpha))\sigma_{n-1}(x)=0.$$

由归纳假设得出特殊的

$$a_1(\sigma_1(\alpha)-\sigma_n(\alpha))=0.$$

因为 $n>1$, σ_1 与 σ_n 是不同的特征标. 因此必有 G 中的一个 α 使得 $\sigma_1(\alpha)\neq\sigma_n(\alpha)$. 由 α 的这样选择必有 $a_1=0$. 将此

用到原来的关系，就由归纳假设也得到 $a_2=a_3=\cdots=a_n=0$.

把这命题应用到 G 是体 E 中乘法群的情况，并且这些特征标是映 E 到 E' 的同构. E 的乘法群就是 E 中所有异于零的元以体的乘法作为运算来理解的.

系 如果 E 与 E' 是两个体，而且 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 是两两不同的映 E 到 E' 的同构，那么 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 是线性无关的.

如果 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 是映体 E 到体 E' 的同构，那么把 E 的元 a 之具有性质 $\sigma_1(a)=\sigma_2(a)=\cdots=\sigma_n(a)$ 者称为在 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 下 E 中的不动点. 其所以选用这种名称，是因为在这些 σ_i 是自同构，而 σ_1 又特别是恒同映射的情况下，就有 $\sigma_i(a)=\sigma_1(a)=a$.

引理 E 的不动点集是 E 的子体. 把它称为关于 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 的不动点体.

因为设 a, b 为不动点，就有

$$\sigma_i(a\pm b)=\sigma_i(a)\pm\sigma_i(b)=\sigma_j(a)\pm\sigma_j(b)$$
$$=\sigma_j(a\pm b),$$

并且

$$\sigma_i(a\cdot b)=\sigma_i(a)\cdot\sigma_i(b)=\sigma_j(a)\cdot\sigma_j(b)=\sigma_j(a\cdot b).$$

从 $\sigma_i(a)=\sigma_j(a)$ 还得到

$$\sigma_i(a^{-1})=(\sigma_i(a))^{-1}=(\sigma_j(a))^{-1}=\sigma_j(a^{-1}).$$

因此，两个不动点的和、差与积仍为不动点，并且不动点的逆元也是不动点.

命题 13 设 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 为两两不同的映体 E 到体 E' 的同构，K 是 E 的不动点体，那么 $(E/K)\geqslant n$.

证 从假定 $(E/K)=r<n$ 来导致矛盾. 设 $\omega_1, \omega_2, \cdots, \omega_r$ 是 K 上的向量空间 E 的一个生成系. 在齐次线性方程

$$\sigma_1(\omega_1)x_1+\sigma_2(\omega_1)x_2+\cdots+\sigma_n(\omega_1)x_n=0,$$
$$\sigma_1(\omega_2)x_1+\sigma_2(\omega_2)x_2+\cdots+\sigma_n(\omega_2)x_n=0,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_1(\omega_r)x_1+\sigma_2(\omega_r)x_2+\cdots+\sigma_n(\omega_r)x_n=0$$

中，未知量个数比方程个数多，所以有非平凡解，记为 x_1, x_2, $\cdots$, x_n. 对 E 中任一元 α, 总可以在 K 中找到元 a_1, a_2, $\cdots$, a_r, 使得 $\alpha=a_1\omega_1+a_2\omega_2+\cdots+a_r\omega_r$. 以 $\sigma_1(a_1)$ 乘第一个方程，$\sigma_1(a_2)$ 乘第二个，等等. 因为 a_i 是不动点，就有 $\sigma_1(a_i)=\sigma_j(a_i)$, 如此得到

$$\sigma_1(a_1\omega_1)x_1+\cdots+\sigma_n(a_1\omega_1)x_n=0,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_1(a_r\omega_r)x_1+\cdots+\sigma_n(a_r\omega_r)x_n=0.$$

把这些方程加起来就有

$$\sigma_1(\alpha)x_1+\sigma_2(\alpha)x_2+\cdots+\sigma_n(\alpha)x_n=0.$$

因为 x_i 不全为零，这个方程是与 σ_1, σ_2, $\cdots$, σ_n 的线性无关相矛盾的.

系 如果 σ_1, σ_2, $\cdots$, σ_n 是体 E 的自同构，并且 K 是 E 中那些经所有 σ_i 作用而不动的元组成的体，那么 $(E/K)\geqslant n$.

证 如果这些 σ_i 之中有恒同映射，就直接得到结论. 如果没有，就把恒同映射加进去，从而得到 $(E/K)\geqslant n+1$.

设 K 是体 E 的子体，σ 是 E 的自同构，如果对于 K 中的每一元 a 总有 $\sigma(a)=a$, 就说 σ 使 K 不变.

设 σ 与 τ 是 E 的两个自同构，把映射 $\sigma(\tau(x))$ 简写成 $\sigma\tau$, 读者不难证实它也是自同构.

[例如 $\sigma\tau(x\cdot y)=\sigma(\tau(x\cdot y))=\sigma(\tau(x)\cdot\tau(y))$
$=\sigma(\tau(x))\cdot\sigma(\tau(y))$].

$\sigma\tau$ 称为 σ 与 τ 之积. 已看到自同构 σ 之逆 σ^{-1} 仍为自同构.

立即得出，由此乘法使得所有自同构的集作成一群.

如果 E 的两个自同构使子体 K 不变，那么其积与逆也使体 K 不变. E 的那些使 K 不变的自同构就作成一群 G. 如果从这个群 G 来决定 G 的不动点体 K'，那么一般只可以说 K 是 K' 的子体.

G. 命题 13 的应用与例子

如下面的一系列例子，命题 13 作出强有力的结论.

1. 设 k 为体. 考虑变量 x 的所有有理函数组成的体 $E=k(x)$. 把 E 中的每个函数 $f(x)$ 映成 $f\left(\frac{1}{x}\right)$ 显然得 E 的一个自同构. 由 $f(x)$ 映成 $f(1-x)$ 也是 E 的自同构. 把这两个自同构用一切方式合成起来，充其量只得六个不同的自同构，即

$$\sigma_1(f(x))=f(x)\text{（恒同映射）},\qquad \sigma_2(f(x))=f\left(\frac{1}{x}\right),$$

$$\sigma_3(f(x))=f(1-x),\qquad \sigma_4(f(x))=f\left(1-\frac{1}{x}\right),$$

$$\sigma_5(f(x))=f\left(\frac{1}{1-x}\right),\qquad \sigma_6(f(x))=f\left(\frac{x}{x-1}\right).$$

所属的不动点体记为 K. K 由满足方程

$$f(x)=f(1-x)=f\left(\frac{1}{a}\right)=f\left(1-\frac{1}{x}\right)=f\left(\frac{1}{1-x}\right)$$
$$=f\left(\frac{x}{x-1}\right)$$

的所有有理函数组成. 只要验证前两个方程就够了，因为其余的都是由这两个产生的结果. 容易看到，函数

$$I=I(x)=\frac{(x^2-x+1)^3}{x^2(x-1)^2}$$

属于 K. 因此 I 的所有有理函数组成的体 $S=k(I)$ 属于体 K.

要证 $K=S$ 并且 $(E/K)=6$. 其实，由命题 13 得到 $(E/K)\geqslant 6$. 因为 $S\subset K$，所以只要证明 $(E/S)\leqslant 6$. 但是 $E=S(x)$. 因此只须找到一个六次方程，其系数为 S 中元，此方程为 x 所满足. 下列方程

$$(x^2-x+1)^3-I\cdot x^2(x-1)^2=0$$

是具有这性质的.

建议读者把这种体的研究作为练习，以便以后能导出所有的中间体.

2. 设 k 为体，$E=k(x_1, x_2, \cdots, x_n)$ 为 n 个变量 $x_1, x_2, \cdots, x_n$ 的所有有理函数组成的体. 如果 $(\nu_1, \nu_2, \cdots, \nu_n)$ 是 $(1, 2, \cdots, n)$ 的一个置换，那么把 E 的每个函数 $f(x_1, x_2, \cdots, x_n)$ 中的 x_1 代以 x_{ν_1}, x_2 代以 x_{ν_2}, $\cdots$, x_n 代以 x_{ν_n}. 由这种方法得到的换 E 成为自身的映射显然是一自同构. 由此作出 $n!$ 个自同构（包含恒同映射在内）. 设 K 为不动点体，即所谓"对称函数"全体组成的集. 命题 13 指出 $(E/K)\geqslant n!$. 现在来考虑多项式

$$f(t)=(t-x_1)(t-x_2)\cdots(t-x_n)=t^n+a_1t^{n-1}+\cdots+a_n,$$

其中

$$a_1=-(x_1+x_2+\cdots+x_n),$$

$$a_2=+(x_1x_2+x_1x_3+\cdots+x_{n-1}x_n),$$

并且一般的 a_i 是 $(-1)^i$ 乘以由 $x_1, x_2, \cdots, x_n$ 中取 i 个不同变量的所有乘积的和. 这些函数 $a_1, a_2, \cdots, a_n$ 称为**初等对称函数**，而 $a_1, a_2, \cdots, a_n$ 的所有有理函数的体 $S=k(a_1, a_2, \cdots, a_n)$ 显为 K 的子集. 与前例相似，要证明 $S=K$，而且 $(E/K)=n!$. 为此只要证 $(E/S)\leqslant n!$. 为此作出下列体序列：

$$S=S_n\subset S_{n-1}\subset S_{n-2}\subset\cdots\subset S_1\subset S_0=E,$$

其中定义

$$S_n=S;\ S_i=S(x_{i+1},\ x_{i+2},\ \cdots,\ x_n)=S_{i+1}(x_{i+1}).$$

只要证明$(S_{i-1}/S_i)\leqslant i$. 因为 S_{i-1} 由 S_i 通过 x_i 的添加得到，就必须找到以 S_i 中元为系数，最高次数为 i 的 x_i 的方程. 所求的多项式为

$$F_i(t)=\frac{f(t)}{(t-x_{i+1})(t-x_{i+2})\cdots(t-x_n)}=\frac{F_{i+1}(t)}{(t-x_{i+1})},$$

并且$F_n(t)=f(t)$. 如果实行常用的（辗转相）除法，那么$F_i(t)$就作为 t 的一个 i 次多项式，其最高项系数为 1，其余系数是变量 $a_1,\ a_2,\ \cdots,\ a_n$ 与 $x_{i+1},\ x_{i+2},\ \cdots,\ x_n$ 的多项式. 在这些表式中只有整数作为系数出现. 显然 x_i 是 $F_i(t)=0$ 的根.

由至今所得结果附带得出$(S_{i-1}/S_i)=i$，所以 S_i 上的向量空间 S_{i-1} 由元 $1,\ x_i,\ x_i^2,\ \cdots,\ x_i^{i-1}$ 生成. 于是，从命题 6 的证明得出，S 上的向量空间 E 就由下列 $n!$ 个元所生成:

(*) $\qquad x_1^{\nu_1}x_2^{\nu_2}\cdots x_n^{\nu_n}$， 其中的每个 $\nu_i\leqslant i-1$.

因此 E 的任一元可唯一地写成以 S 中元为系数的这 $n!$ 个元的一个线性组合. 如果 E 中一元是 $x_1,\ x_2,\ \cdots,\ x_n$ 的多项式，那么将进而证明其系数也是 $a_1,\ a_2,\ \cdots,\ a_n$ 的多项式. 假定这个已得到证明，通常形式的对称函数主要命题便作为它的特例得以证明. 这个主要命题是说，不动点体 K 中的多项式 $g(x_1,\ x_2,\ \cdots,\ x_n)=g$ 也可以写成 $a_1,\ a_2,\ \cdots,\ a_n$ 的多项式. 由于 $K=S$，g 就可以浅显地写成(*)的元的线性组合，其中除了属于 $\nu_1=\nu_2=\cdots=\nu_n=0$ 的这一项外，所有项的系数为 0，g 自身作为这项的系数. 如果上述的命题证明了，那么由表示的唯一性得出，g 就是 $a_1,\ a_2,\ \cdots,\ a_n$ 的多项式.

为了证明这个附带的命题，设 $g(x_1,\ x_2,\ \cdots,\ x_n)$ 是 E 的

任一多项式．因为 $F_1(x_1)=0$ 是 x_1 的一次方程，x_1 就可以表成 a_i 与 $x_2, x_3, \cdots, x_n$ 的多项式．把这表式引到 $g(x_1, x_2, \cdots, x_n)$ 里．由 $F_2(x_2)=0$ 就可以把 x_2^2 或更高的幂表成 $x_2, x_3 \cdots, x_n$ 与 a_i 的多项式，可是，其中 x_2 的最高幂不过只有 1 次幂出现．由 $F_3(x_3)=0, x_3^3$ 与 x_3 的高次幂可表成 $x_3, x_4, \cdots, x_n$ 与 a_i 的多项式，其中 x_3 最高不过二次，如果把这些表式代入 $g(x_1, x_2, \cdots, x_n)$ 就看到它可写成 x_ν 与 a_ν 的多项式，其中 x_i 的次数是低于 i 的．因此，$g(x_1, x_2, \cdots, x_n)$ 就是(*)中那 $n!$ 个项的线性组合．但是这些项的系数而今都是 a_i 的多项式了．

H．正规的体扩张

回到命题 13 的系所述的情况．如此，设 E 为体，$\sigma_1, \sigma_2, \cdots, \sigma_n$ 为 E 的自同构，并设 K 是 E 中所有这样的元组成的子体，其中每个元由每个 σ_i 映成自身．已证 $(E/K)\geqslant n$．如果这些 σ_i 组成的集 G 并不是群，那么，或者有两个 σ_i 的积是新的元，要不，就有一个 σ_i 的逆元是新的元，即 E 的新的自同构．如果把它加入这些 σ_i 中，那么 K 自身不变，因此得到 $(E/K)\geqslant n+1$．因此，命题 13 的系中等号是不成立的．所以，从现在起假设 G 作成一个群．于此情况中，起一定作用的是 E 中 α 的这个函数

$$S(\alpha)=\sigma_1(\alpha)+\sigma_2(\alpha)+\cdots+\sigma_n(\alpha).$$

如果把一个 σ_i 作用于 $S(\alpha)$，就得到这样的和

$$\sigma_i\sigma_1(\alpha)+\sigma_i\sigma_2(\alpha)+\cdots+\sigma_i\sigma_n(\alpha).$$

因为 G 是群，这些自同构 $\sigma_i\sigma_1, \sigma_i\sigma_2, \cdots, \sigma_i\sigma_n$ 不过是 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 的置换序列．这就指出 $S(\alpha)$ 经过所有的 σ_i 而不动，因此它属于 K．$S(\alpha)$ 这函数也称为 α 的迹，它不恒等于零，否则就与 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 的线性无关性矛盾．现在来证明

命题 14 如果 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 作成体 E 的自同构群，并且 K 是所属的不动点体，那么 $(E/K)=n$.

证 由命题 13 就只要证明：E 的 $n+1$ 个元 $\alpha_1, \alpha_2, \cdots, \alpha_{n+1}$ 对于 K 总是线性相关的. 为此来考虑下列 E 中线性齐次方程组：

$$
\begin{aligned}
&x_1\sigma_1^{-1}(\alpha_1)+x_2\sigma_1^{-1}(\alpha_2)+\cdots+x_{n+1}\sigma_1^{-1}(\alpha_{n+1})=0,\\
&x_1\sigma_2^{-1}(\alpha_1)+x_2\sigma_2^{-1}(\alpha_2)+\cdots+x_{n+1}\sigma_2^{-1}(\alpha_{n+1})=0,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&x_1\sigma_n^{-1}(\alpha_1)+x_2\sigma_n^{-1}(\alpha_2)+\cdots+x_{n+1}\sigma_n^{-1}(\alpha_{n+1})=0.
\end{aligned}
$$

因为未知量个数多于方程个数，就有非平凡解. 设有 $x_1\neq 0$. 因为这些方程还可乘以 E 中任一因子，就能使得 x_1 是 E 中的、其迹非零的元. 于是分别以 σ_i 作用于第 i 个方程. 结果为

$$\sigma_i(x_1)\alpha_1+\sigma_i(x_2)\alpha_2+\cdots+\sigma_i(x_{n+1})\alpha_{n+1}=0.$$

对 i 求和，得到

$$S(x_1)\alpha_1+S(x_2)\alpha_2+\cdots+S(x_{n+1})\alpha_{n+1}=0.$$

因为 $S(x_\nu)$ 属于 K，而 $S(x_1)\neq 0$，所述的线性相关性已得证.

系 1 在命题 14 中的同样条件下得到：使体 K 不变的 E 的自同构 σ 必属于 G.

证 如果 σ 不同于所有的 σ_i，把这 σ 加入 G. K 不变，由命题 13 得到 $(E/K)\geqslant n+1$，与命题 14 矛盾.

由此立即得到

系 2 E 的不同的自同构群有不同的不动点体.

定义 如果 K 为其扩体 E 的有限自同构群的不动点体，那么扩体 E 称为体 K 的**正规扩张**.

设 $f(x)$ 为 K 中多项式，如果其不可约因子没有重根，那么 $f(x)$ 称为**可分的**. 设 E 为体 K 之一扩张，α 为 E 中的

元，如果 α 是 K 中一可分多项式 $f(x)$ 之一根，那么 E 的这个元 α 称为**可分的**．如果 E 的每个元都是可分的，E 就称为 K 的**可分扩张**．

命题 15 设 E 是具有群 G 的、K 上的正规扩张．那么 E 就是 K 的可分扩张．更精确的是：设 α 是 E 的元，如果 α 在 G 的这 n 个自同构作用下所得两两不同的象是 α_1，α_2，$\cdots$，α_r，那么多项式

$$p(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$$

就是 K 中的以 α 为其根的不可约多项式．

证 把 G 的这 n 个元都乘以 σ_i，那就得到 G 的所有元．这就指出，r 个元

$$\sigma_i(\alpha_1),\ \sigma_i(\alpha_2),\ \cdots,\ \sigma_i(\alpha_r)$$

不过是 α_1，α_2，$\cdots$，α_r 这些元的一个置换．因此 $p(x)$ 的系数经 σ_i 作用不变．于是 $p(x)$ 就是 K 中多项式，而且 $p(x)$ 显然是可分的．因为 α 自身出现在 α 的这些象之中，$p(x)$ 就有根 α．如果 K 中有以 α 为其根的某个多项式 $f(x)$，那么也有 $\sigma_i(f(\alpha))=0$，从而 $f(\sigma_i(\alpha))=0$．所以 $f(x)$ 也具有根 α_1，α_2，$\cdots$，α_r，因此可被 $p(x)$ 整除．这就指出 $p(x)$ 的不可约性，完满地证明了本命题．

系 设 E 是 K 的正规扩张，$p(x)$ 为有根 α 在 E 中的 K 中不可约多项式．那么 $p(x)$ 在 E 中得分解成纯为线性的因子．

证 由于属 α 的不可约多项式的唯一性，$p(x)$ 就应当是那个在命题 15 所作的多项式，它显然在 E 中分解成纯为线性的因子．

命题 16 设 E 是具有群 G 的、K 上的正规扩张，B 为中间体．则 E 为 B 的正规扩张，其自同构群 U 由 G 中那些使

体 B 不变的自同构组成.

证 设 U 为由 G 中那些使得体 B 不变的自同构组成的子群. 把群 U 的阶记为 r, 设 U 的不动点体为 B'. 于是 $B\subset B'$, 从而应当证明 $B=B'$. 今有 $(E/B')=r$, 因此 $(E/B)\geqslant r$, 从而只要证明 $(E/B)=r$. 把 G 的自同构 σ_i 作用于 B 上, 就把 B 映成其同构象. 然而可能有不同的自同构作用在 B 上产生相同映射. 即如对 B 中所有元 β 都有 $\sigma_i(\beta)=\sigma_j(\beta)$. 这就等价于 $\sigma_i^{-1}\sigma_j(\beta)=\beta$, 因此等价于这 $\sigma_i^{-1}\sigma_j$ 是属于 U 的. 也就是等价于 σ_j 属于旁系 σ_iU. 因此, 一个旁系 σ_iU 的元正好就是那些作用于体 B 上产生相同同构的元. 因此如果设 $n=rs$, 那么 s 就是这些旁系的个数. 于是 G 的元作用于 B 上就正好产生 s 个不同的同构映射. 一方面, 这 s 个不同映射的不动点体当然是体 K, 另一方面, 由命题 13 知道, 必有 $(B/K)\geqslant s$. 两个不等式 $(E/B)\geqslant r$, $(B/K)\geqslant s$ 相乘得出 $(E/K)\geqslant n$. 既然此处的等号是成立的, 前两个不等式中的等号也必定成立. 于是 $(E/B)=r$, $(B/K)=s$. 命题便完全证明了.

由此证明引起, 对于每个在 K 上具有次数 s 的中间体 B, 在 E 中显然有 B 的 s 个不同的同构, 它们使得 K 的每个元都不动, 而且每个这样的同构是由 G 之一元所产生. 容易看到, 在 E 的任一扩体中, 绝不会有使 K 每元不动的 B 的更多的同构. 否则, 把它加入 s 个已知的同构之中. K 就是这 $s+1$ 个同构的不动点体, 那么由命题 13 就必定会得出次数 $(B/K)\geqslant s+1$.

如上已知, 属于 G 的每一子群 U 就有一个中间体 B, 即 U 的不动点体(包含 K 的). 不同的子群由命题 14 的系 2 便导出不同的中间体. 最后, 由命题 16 指出, 每个中间体 B 是

G 的一个子群 U 的不动点体．因此，这些子群与中间体的对应是一一的．

如果 U_1 与 U_2 是分别以 B_1 与 B_2 为其不动点体的子群，而且 $U_1 \subset U_2$，那么显然 $B_1 \supset B_2$．如果 $B_1 \supset B_2$，那么使 B_1 不变的每一自同构就也使 B_2 不变；因此得到 $U_1 \subset U_2$．于是，上述对应使包含关系相反．最后，由此对应使整个群 G 对应于体 K，仅由恒同元组成之子群对应于整个体 E．因此，为了描述这些中间体，便可利用它们所属的 G 的子群．现用实例说明如下：

设 B 为中间体，它所属的子群为 U，σ 为 G 之一元．由 σ 的作用得 B 的象 $\sigma(B)$ 为一中间体．要求 $\sigma(B)$ 所属的子群．$\sigma(B)$ 的元具形式 $\sigma(\beta)$，其中 β 属于 B．必须从 G 中求得这样的元 τ 使得每个 $\sigma(\beta)$ 都不动，因此就是 $\tau\sigma(\beta)=\sigma(\beta)$．此方程与 $\sigma^{-1}\tau\sigma(\beta)=\beta$ 等价，而这就是说，$\sigma^{-1}\tau\sigma$ 属于 U，于是 τ 自身便属于 $\sigma U\sigma^{-1}$．因此 $\sigma U\sigma^{-1}$ 就是 $\sigma(B)$ 所属的群．

立刻可以判断在什么条件下 B 是 K 的正规扩张．如果 $(B/K)=s$，就已看到一般只可能有 B 的 s 个同构（使 K 不变的）在 E 的扩体之中，而所有这些个同构都是由 G 中之元所产生的．如果 B 在 K 上是正规的，那么另一方面就必定有 B 的 s 个自同构，因此每个同构就必定是 B 的自同构．于是对于 G 中所有的 σ 必有 $\sigma(B)=B$．按上所述就是说，对于 G 中所有的 σ 都有 $\sigma U\sigma^{-1}=U$．这种子群 U 如众所周知称为 **G 的正规子群**．因此，如果 U 是 G 的正规子群，那么 B 就正好是 K 的正规扩张．

现在假设中间体 B 是 K 的正规扩张，因此 U 便是 G 的正规子群．每个使 K 不变的 B 的自同构因此就是由 G 之一元 σ 作用于 B 上产生的．既然旁系 σU 的每一自同构作用于

B 上产生与 σ 生成的自同构相同，所求的 B 的那些自同构便与那些旁系 σU 有一一对应关系．如果 σU 与 τU 是两个这样的旁系，那么它们就相当于分别以 σ 与 τ 作用于 B 上所得的自同构．所以它们的合成由处于旁系 $\sigma\tau U$ 中的自同构 $\sigma\tau$ 得到．因为 U 是正规子群，这旁系 $\sigma\tau U$ 就是 σU 与 τU 的积．看到 B 的那些自同构的合成一如那些旁系．正规子群 U 的旁系群称为**商群** G/U．因此，在这种意义下 K 的正规扩张 B 具有自同构群 G/U．

总结起来便证明了

命题 17（基本命题） 设 E 是具有群 G 的、K 上的正规扩张．把 G 的每个子群 U 对应于它的不动点体 B，那么由此就在子群与中间体之间有了一个一一对应．此对应使包含关系相反．对于一个给定的中间体 B 所属的群，是由 G 中那些使 B 不变的元所组成的．$(E/B)=U$ 的阶，$(B/K)=G$ 中 U 的指数＝旁系个数．在 E 的扩体中，使 K 中元不动的 B 的每个同构可由 G 之一元 σ 作用于 B 上而得到，其中旁系 σU 所有元总产生 B 的相同同构．如果 U 是 G 的正规子群，那么 B 就正好是 K 的正规扩张．在这种情况下此扩张 B 的自同构群就是商群 G/U．

现在为了 E 是 K 的正规扩张需要求得一个简单的条件．把它叙述为

命题 18 如果 E 是 K 中一个可分多项式 $p(x)$ 的分裂体，那么 E 就正好是 K 的正规扩张[1]．

证 1．设 E 是 K 的正规扩张，$\omega_1, \omega_2, \cdots, \omega_n$ 是 K 上的向量空间 E 的生成系．设 $p_i(x)$ 是以 ω_i 为根的 K 中不可

1) “如果…，那么…就正好是…”是口语直译．其实，这就是说：前一句的充要条件为后一句的“E 是 K 的正规扩张”．以后有此口语即如此了解．——译者

约多项式．已知 $p_i(x)$ 是可分的而且在 E 中完全分解成线性因子．取

$$p(x)=p_1(x)p_2(x)\cdots p_n(x).$$

于是，$p(x)$ 是可分的而且在 E 中分解成纯为线性的因子．因为所有的 ω_i 都在 $p(x)$ 的根中出现，其分裂体正好就是 E．

2．设 $p(x)$ 为 K 中可分多项式，E 是它的分裂体．设群 G 是 E 的所有使 K 不变的自同构．因为 (E/K) 有限，由命题 13 的系，G 便也是有限群．只要证明，凡经 G 的所有元作用而不动的 E 中元 θ，必定是属于 K 的元；因为如此 K 就是 G 的不动点体了．如果 $p(x)$ 的根都在 K 中，就有 $E=K$，上述显然为真．因此假设 $p(x)$ 正好有 n 个不在 K 中的根，其中 $n\geqslant 1$．还假设对所有那些不在 K 中的根数较 n 为少的 $p(x)$，上述已得证明．设 α_1 为 $p(x)$ 之一根，它不在 K 中，并设 $p_1(x)$ 为 K 中的以 α_1 为根的不可约多项式．因为 $p(x)$ 可分，$p_1(x)$ 就没有重根．用 $K(\alpha_1)$ 代替基体 K．于是 $p(x)$ 为此体的可分多项式，并且 E 仍为其分裂体．而今 $p(x)$ 不在 $K(\alpha_1)$ 中的根数已较 n 为少．因此，由归纳假设，E 便是 $K(\alpha_1)$ 的正规扩张．使 $K(\alpha_1)$ 不变的 E 的那些自同构所组成的群 U 于是就有 $K(\alpha_1)$ 作为其不动点体，并且 U 是 G 的子群．已设 θ 为经 G 中所有自同构作用不变之元．它当然经 U 中所有自同构作用也是不变的，从而也就属于 $K(\alpha_1)$．设 $p_1(x)$ 的次数为 s，于是 θ 具形式

$$(**)\qquad \theta=c_0+c_1\alpha_1+\cdots+c_{s-1}\alpha_1^{s-1},$$

其中所有的 c_i 都在 K 中．

另一方面，$p_1(x)$ 无重根．把 $p_1(x)$ 的根记为 $\alpha_1, \alpha_2, \cdots, \alpha_s$．根据命题 8，就有映 $K(\alpha_1)$ 成 $K(\alpha_i)$ 的同构 σ_i，其中 K 的元按序不动，而 α_1 则换成 α_i．σ_i 把 $p(x)$ 换成 $p(x)$．体 E 为

在 $K(\alpha_1)$ 上的、$p(x)$ 的分裂体，从而也是在 $K(\alpha_i)$ 上的、$p(x)$ 的分裂体．根据命题 10，同构 σ_i 可拓展为映 E 成 E 的同构 τ_i，所以这 τ_i 就是 G 之一元，于是 θ 经 τ_i 作用也是不动的．把 τ_i 作用于(**)，得到

$$\theta = c_0 + c_1\alpha_i + \cdots + c_{s-1}\alpha_i^{s-1}.$$

于此，多项式 $c_{s-1}x^{s-1} + c_{s-2}x^{s-2} + \cdots + c_1x + (c_0 - \theta)$ 就有了 s 个互不相同的根 $\alpha_1, \alpha_2, \cdots, \alpha_s$．根数比次数多，那么所有的系数，尤其是常数项就应当为零．因此 $\theta = c_0$，即为 K 之一元．

关于自同构的算法，还给些附注．由实际选择的生成系来描述 K 的正规扩张 E，$E = K(\alpha_1, \alpha_2, \cdots, \alpha_r)$．就是说，每个元 θ 是以 K 中元为系数、$\alpha_1, \alpha_2, \cdots, \alpha_r$ 的有理函数．如果知道 G 中元 σ 作用于 E 的生成元 α_i 所得效果，那么这就正好把 σ 描绘出来了．因此，通过所有 $\sigma(\alpha_i)$ 的指示便确定了 σ．如果对于 α_i 知道在 K 中有以 $f(\alpha_i) = 0$ 的多项式 $f(x)$，那么经 σ 作用必得 $f(\sigma(\alpha_i)) = 0$．于是 $\sigma(\alpha_i)$ 必定是 $f(x)$ 所必有的根．例如，E 是不具重根的一个多项式的分裂体，并设 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 就是这些根，那么可把这些 α_i 取为 E 的生成系，从而知道 σ 把这些根排成一个一定的置换．按上所述(但是不在所有情况下都是实用的)，因此可以把 G 看作一个一定的置换群.

用一个例子来说明上述，细节让读者自己去讨论．设 K 为有理数体，E 为多项式 $x^4 - 2$ 的分裂体．因为由上注明，如何作分裂体是无关紧要的，从复数体来讨论根，其中 $x^4 - 2$ 就有这些零点

$$\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -i\sqrt[4]{2}.$$

E 含有 $\sqrt[4]{2}$，也含有 i．这两个元就是 E 的实际生成系．多

项式在 K 中不可约，因此得到

$$(K(\sqrt[4]{2})/K)=4.$$

因为 $K(\sqrt[4]{2})$ 只含实数，x^2+1 在 $K(\sqrt[4]{2})$ 中是不可约的，从而就看到 $(E/K)=8$. 作为一个可分多项式的分裂体，E 就是可分扩张，因此正好具有 8 个自同构. 对于 $\sqrt[4]{2}$ 的象占有四个可能性，对于 i 的象占有两种. 因此看到在这种情况下，对于 $\sqrt[4]{2}$ 与 i 的象的所有 8 个组合实际上就提供了一些自同构. 如果把那个换 $\sqrt[4]{2}$ 为 $i\sqrt[4]{2}$ 而使 i 不动的自同构记为 σ; 使 $\sqrt[4]{2}$ 不动而换 i 为 $-i$ 的自同构记为 τ. 容易算得这 8 个自同构如下：

$$1,\ \sigma,\ \sigma^2,\ \sigma^3,\ \tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau$$

（这儿的 1 指恒同映射）. 还得出 $\sigma^4=1$, $\tau^2=1$ 以及 $\tau\sigma\tau^{-1}=\sigma^{-1}$. 由此读者可以认识，这个群与一个正方形在三维空间中的旋转群是同构的. K 上的向量空间 E 由元

(***) $$1,\ \sqrt[4]{2},\ (\sqrt[4]{2})^2,\ (\sqrt[4]{2})^3,$$
$$i,\ i\sqrt[4]{2},\ i(\sqrt[4]{2})^2,\ i(\sqrt[4]{2})^3$$

所生成. 一个有用的练习是来决定 G 的所有的子群，并且对每个子群来作出属于它的中间体. 属于子群 U 的中间体几乎可如下来决定：把一个元 θ 写成带有待定系数的、(***)的那些元的线性组合，如果对 U 中每个元 λ 来计算 $\lambda(\theta)$，从而求出使得对 U 中所有的 λ 都有 $\lambda(\theta)=\theta$ 的那些条件. 如此便求得两个中间体，再也找不出更多的了.

I. 代数扩张和可分扩张

如果体 E 中每一元都是体 K 的代数元，E 就称为 K 的**代数扩张**.

命题 19 如果 (E/K) 是有限的，那么 E 就是 K 的代数

扩张.

证 设$(E/K)=n$，并且α为E的元. 于是$1, \alpha, \alpha^2, \cdots, \alpha^n$这$n+1$个元在$K$上线性相关，而这样的线性相关性给出了以$K$中元为系数的$\alpha$的一个方程.

现在设E是由K通过有限个代数元$\alpha_1, \alpha_2, \cdots, \alpha_r$的添加而得到的扩张. 在体链$K\subset K(\alpha_1)\subset K(\alpha_1, \alpha_2)\subset\cdots\subset K(\alpha_1, \alpha_2, \cdots, \alpha_r)=E$中，每个体对其前邻都具有有限的次，所以$(E/K)$也是有限的. 因此$E$是$K$上的代数扩张. 如果$E$是由$K$通过无穷多个代数元的添加而得到的扩张，那么每一单个的元就已在一个子体之中，这子体是由有限个代数元添加于K所得，因此就是K的代数扩张. 故得

命题 20 凡通过代数元添加于K所生成的扩张总是代数扩张.

此外还要论证

命题 21 设$K\subset E_1\subset E_2$，其中E_1为K的代数扩张，E_2是E_1的代数扩张. 那么E_2便是K的代数扩张.

证 设α为E_2的元. 由假设，α满足E_1中一个代数方程，设其系数为$\alpha_1, \alpha_2, \cdots, \alpha_r$. 于是$\alpha$为体$E'=K(\alpha_1, \alpha_2, \cdots, \alpha_r)$上的代数元. 因此，体$E'(\alpha)$在$E'$上的次数是有限的. E'在K上的次数有限，所以$(E'(\alpha)/K)$就是有限的. 由此得知α是K上的代数元.

设$E=K(\alpha_1, \alpha_2, \cdots, \alpha_r)$，而且每个$\alpha_i$在$K$上都是可分的. 因此$K$中以$\alpha_i$为根的不可约多项式$p_i(x)$无重根. 取$f(x)=p_1(x)p_2(x)\cdots p_r(x)$，把$E$上的$f(x)$的分裂体记作$E'$. 于是$E'$也是$K$上的$f(x)$的分裂体，并把$E$作为中间体包含其中. 由命题18，$E'$是$K$的正规扩张. 因此，由命题15，$E'$是$K$的可分扩张，从而$E$也是$K$的可分扩张. K的正规扩

张 E' 只有有限个中间体，就是自同构群所有子群的个数．因此在 K 与 E 之间也只有有限个体．由此得

命题 22 设 $E=K(\alpha_1, \alpha_2, \cdots, \alpha_r)$，而且每个 α_i 在 K 上都是可分的．那么 E 是 K 的可分扩张，并且只有有限个体在 K 与 E 之间．可以把 E 扩张到 K 上的正规扩体 E'．

引理 设 σ 为映 K 成 K' 的同构，$p(x)$ 是 K 中的无重根多项式，$p'(x)$ 为其 σ 象．那么 $p'(x)$ 也无重根．

证 设 E 是 K 上 $p(x)$ 的分裂体，E' 是 K' 上 $p'(x)$ 的分裂体．由命题 10，σ 可开拓为映 E 成 E' 的同构 τ．E 中 $p(x)$ 的线性因子分解经 τ 的作用便得到 E' 中 $p'(x)$ 分解成不同的线性因子．

命题 23 设 $K\subset E_1\subset E_2$，其中 E_1 在 K 上可分，E_2 在 E_1 上可分，并且都是有限次．那么 E_2 在 K 上可分．

证 设 α 为 E_2 的元，而且 $p(x)$ 是其所属的、E_1 中的不可约多项式．由假设，$p(x)$ 无重根．把 E_1 扩张到 K 上的正规扩体 E，其自同构群记以 G．设 E 中 $p(x)$ 的不可约因子为 $p_1(x), p_2(x), \cdots, p_r(x)$．它们互不相同而且都无重根．把 G 所有自同构作用在这些多项式上．如此得到的那些不同的多项式记为 $q_1(x), q_2(x), \cdots, q_s(x)$．因此每个 $q_i(x)$ 为一 $p_j(x)$ 的象．由上引理知每个 $q_i(x)$ 无重根．因为对给定的根其不可约方程的唯一性，没有两个 $q_i(x)$ 具公根．这些 $q_i(x)$ 由 G 的一个自同构 σ 作用得到 s 个互不相同的象，由 G 的群的性质，这 s 个象多项式中的每个仍是一 $p_j(x)$ 的象．因此看到 σ 只不过置换这些多项式 $q_i(x)$．取 $f(x)=q_1(x)q_2(x)\cdots q_s(x)$，那么 $f(x)$ 便是经 G 作用而系数不变的多项式，因此这些系数属于 K．$f(x)$ 无重根而且可被 $p(x)$ 整除，正是因为每个 $p_i(x)$ 都出现在这些 $q_j(x)$ 之中．由此得 $f(\alpha)=0$，从而 α 在 K 上

是可分的.

现在要讨论通过一个单独的代数元 α 的添加可以得到的体扩张. 这种扩张称为**单纯的**, α 这元称为**本原元素**. 现在来证明

命题 24 具有有限次数的 K 的扩张 E, 它为单纯的充要条件是只有有限个中间体存在.

证 1. 设 $E=K(\alpha)$ 为单纯扩张, $p(x)$ 为属于 α 的、K 中以 1 为最高系数的不可约多项式. 设 B 为一中间体, $p_1(x)$ 为属于 α 的、B 中以 1 为最高系数的不可约多项式. 于是 $p_1(x)$ 为 $p(x)$ 的因子, 因此对于所有的中间体 B 只能有有限个 $p_1(x)$. 设 K 通过 $p_1(x)$ 所有系数的添加而成的中间体为 B_0. 就有 $B_0\subset B$, 而且如果随后证明了 $B_0=B$, 那就得出只能有有限个 B. 为此只须证明 $(E/B)\geqslant(E/B_0)$. 而今 $p_1(x)$ 也是 B_0 的多项式, 以 α 为其根. 因为 $E=B_0(\alpha)=B(\alpha)$, (E/B_0) 最高不过是 $p_1(x)$ 的次数, 至于这次数却是等于 (E/B) 的.

2. 设 E 是 K 的具有有限次数的扩张, 只有有限个中间体. 但是还得作个补充的假定, 就是设 K 含有无穷多个元. 设 α 与 β 是 E 中的两个元. 对 K 中的每个元 c, 作元 $\gamma_c=\alpha+c\beta$, 以及单扩张 $K_c=K(\gamma_c)$. 所有的 K_c 都是中间体. 因为只有有限个中间体, 而对于 c 却有无穷多个可能, 就可以这样决定 c 与 d, 使得 $c\neq d$ 而正好 $K_c=K_d$. γ_d 与 γ_c 同在 K_c 之中, 所以其差 $(c-d)\beta$ 也一样在 K_c 之中. 由此得出 β 在 K_c 之中, α 也是如此, 因此 $K(\alpha,\beta)\subset K_c$. 因为 $K_c\subset K(\alpha,\beta)$, 就有 $K(\alpha,\beta)=K(\gamma_c)$. E 中两元对 K 的添加于是可以一元的添加来代替. 现在因为 E 是可由 K 通过有限个元(例如 K 上的向量空间 E 的生成系)的添加而得到

的，所以 E 就是 K 的单纯扩张.

3. 如果 K 只含有限个元而且 E 为其具有限次数的扩张，因此 E 也只含有限个元. 对此情况的证明于下节给出.

系 如果 E 是 K 的具有有限次数的可分扩张，那么 E 是单纯扩张.

证 由命题 22，只有有限个中间体的原故.

还考虑体的一些简单性质. 从体的具体的例子出发. 熟知的有理数体记作 Q. 进一层的体可以由数论初步来了解:

设 p 为一寻常的素数. 于是可以把整数集分成模 p 的同余类. 这些同余类之间的加法与乘法定义为其代表的加与乘. 这 p 个同余类按上述运算作成的体记为 Q_p. 因为由初等数论的命题，如果 a 不能被 p 整除，同余式 $ax\equiv b \pmod p$ 有唯一解.

设 K 为任一体. 现在来研究 K 的加法群. 与乘法群中元的幂 a^n 相类似，加法群有元的倍 na. 乘法群中元 a 的阶就是使 $a^n=1$ 的那个(如果存在)最小正整数 n，与此类似，加法群中元 a 的阶便是使 $na=0$ 最小正整数 n. 而今申明 K 中异于零的所有元都有相同的加法阶. 因为由 $na=0$ 即得 $na\cdot a^{-1}b=0$，因此对每个 b 就有 $nb=0$. 如果 K 中异于零的所有元都有有限阶 p，那么 p 必为素数. 因为如有 $p=rs$，其中 $r<p$ 且 $s<p$，那么 $sa\neq 0$ 这元就会有较小的阶 r 了. 上述情况的 K 称为有特征 p 的体. 如果异于零的元没有有限的阶，那么 K 就称为有特征 0 的. 如此称呼之所以合理，是因为在具有某特征的体中，下面的声明总是对的:

设 n 为整数，a 为 K 之一元，那么 $na=0$ 之成立，正好是在: 或者 $a=0$; 要不 n 就是特征的倍数.

为了使 K 的单位元素与数 1 有所区别，记前者为 e. 设

K 是特征 $p>0$ 的体. 因为 e 具有加法阶 p, e 的倍只产生 K 中 p 个不同的元, 并且 $me=ne$ 正好是在 n 与 m 属于模 p 的同一个同余类时成立. 因此, e 的倍与模 p 的同余类一一对应. 这些倍的加法 $ne+me=(m+n)e$ 与乘法 $ne\cdot me=nme^2=nme$ 又分别对应其所属同余类的加与乘. 因此, e 的倍作成与 Q_p 同构的体. 通常只写 n 来代替 ne, 应当注意, 此后 n 只取作模 p 的. 于是也说 e 的倍构成体 Q_p. 这种意义下的 Q_p 就是 K 的子体. 因为 K 的子体必含 e, 所以也含 e 的倍, 从而 Q_p 是 K 的最小子体.

仍设 K 为特征 $p>0$ 的体. 对于 $1\leqslant i\leqslant p-1$, 二项式系数 $\binom{p}{i}=\frac{p!}{i!(p-i)!}$ 的分母既不能被素数 p 整除, 分子却不然, 可见这系数就是个能为 p 整除的整数. 把 $(a+b)^p$ 按二项命题展开, 那么所有的中间项 $\binom{p}{i}a^ib^{p-i}$ 便消失了, 得到

$$(a+b)^p=a^p+b^p.$$

由于还有

$$(ab)^p=a^pb^p,$$

故得, 把 K 中每个元映成其 p 幂所得到的映 K 到本身的映射, 就是同构映射. 尤其还看到

$$(a-b)^p=a^p-b^p.$$

因此这映射是一一的: 由于 $a^p=b^p$ 得到 $a=b$. 随着举个映 K 成 K 的同构的例, 如 K 只含有限个元(由于这映射是一一的). 在这种情况因此作出了 K 的一个自同构.

现在设 K 具有特征 0. e 的倍 ne 就都是互不相同的. 因为 K 是个体, K 也含所有的商 $\frac{ne}{me}$, 假设是 $m\neq 0$. 两个商相等 $\frac{ne}{me}=\frac{n'e}{m'e}$ 等价于 $nm'e=n'me$, 因此等价于 $nm'=mn'$,

从而等价于 $\frac{n}{m}=\frac{n'}{m'}$. 如果把有理数 $\frac{n}{m}$ 对应于商 $\frac{ne}{me}$，那么在有理数与商之间便定义了一一对应. 由此，读者自己容易证实，有理数的和与积分别对应于其对应商的和与积. 这种对应因此产生了有理数体 Q 与商 $\frac{ne}{me}$ 集的同构. 一如既往对于特征 $p>0$ 的情况，于此也通常把 $\frac{ne}{me}$ 与有理数 $\frac{n}{m}$ 看成一样的，因此，而今 Q 便是 K 的最小子体了.

微分　设 $f=f(x)=a_0+a_1x+\cdots+a_nx^n$ 为体 K 中的多项式，于是定义 $f'=a_1+2a_2x+\cdots+na_nx^{n-1}$. 读者也能容易证实，对于任何两个多项式 f 与 g，总有

$$(f+g)'=f'+g',$$

$$(f\cdot g)'=fg'+g'f,$$

$$(f^n)'=nf^{n-1}\cdot f'.$$

命题 25　K 中的多项式 f 有重根的充要条件是：在分裂体 E 中这两个多项式 f 与 f' 有公根. 这个条件等价于：体 K 中的 f 与 f' 有高于零次的公因子.

设 α 是 $f(x)$ 的重数为 k 的根，那么

$$f=(x-\alpha)^kQ(x)，\text{其中 } Q(\alpha)\neq 0.$$

由此得

$$\begin{aligned} f'&=(x-\alpha)^kQ'(x)+k(x-\alpha)^{k-1}Q(x)\\ &=(x-\alpha)^{k-1}[(x-\alpha)Q'(x)+kQ(x)]. \end{aligned}$$

如果 $k>1$，那么 α 是 f' 的具有重数至少为 $k-1$ 的根. 如果 $k=1$，那么 $f'(x)=Q(x)+(x-\alpha)Q'(x)$，从而 $f'(\alpha)=Q(\alpha)\neq 0$. 由此 f 与 f' 有 α 为其公根的充要条件是：α 是 f 的具有重数至少为 2 的根.

如果 f 与 f' 有公根 α，那么 K 中的以 α 为根的不可约

多项式同时为 f 与 f' 的因子. 反之, f 与 f' 的公因子之任一根同时为 f 与 f' 的根.

系 1 K 中不可约多项式 $f(x)$ 无重根的充要条件是: $f'(x)$ 不是零多项式.

证 如果 $f'(x)$ 不是零多项式, 那么它有低于 $f(x)$ 的次数. 因此, $f(x)$ 与 $f'(x)$ 的公因子也有小于 $f(x)$ 的次数. 因为 $f(x)$ 不可约, 这种公因子就只能是常数. 于是 $f(x)$ 无重根. 然而, 如果 $f'(x)$ 是零多项式, 那么 $f(x)$ 本身就是 $f(x)$ 与 $f'(x)$ 的公因子, 因此 $f(x)$ 有重根.

系 2 如果 K 具有特征 0, 那么每个多项式都是可分的.

证 于此情况以 0 为其导数的唯一多项式就是常数. 因此每个不可约多项式只有单根.

注 如果 K 具有特征 $p>0$, 那么存在不是常数的多项式, 例如 x^p, 其导数为 0.

J. Abel 群及其在体论上的应用

往往体的有限子集对于体乘法构成群. 这种群结构甚为简单:

命题 26 体的乘法群的有限子群 S 总是循环的.

其证明是根据下列涉及 Abel 群的引理:

引理 1 如果 Abel 群中元 A 的阶为 a, 元 B 的阶为 b, 而且 c 是 a 与 b 的最小公倍, 那么群中就有以 c 为阶的元 C.

证 (a) 如果 a 与 b 互素, 那么 $C=AB$ 即所求的以 c 为阶的元.

其实, 如果 $C^r=1$, 就得到 $C^{rb}=A^{rb}B^{rb}=A^{rb}=1$, 因此 rb 可被 a 整除, 从而 r 可被 a 整除. 同法可证得 r 可被 b 整除, 所以也可被 ab 整除. 另一方面, $C^{ab}=1$, 因此 ab 就是 C 的阶.

(b) 如果 d 为 a 的因子，那么群中有以 d 为阶的元. 显然 $A^{\frac{a}{d}}$ 就是一个这样的元.

(c) 现在考虑一般情况. 设 $p_1, p_2, \cdots, p_r$ 为或者整除 a、要不就整除 b 的所有素数，并设

$$a=p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r},$$

$$b=p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}.$$

两个数 n_i 与 m_i 中较大的记为 t_i. 于是

$$c=p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}.$$

由(b)，群中有以 $p_i^{n_i}$ 为阶的元，也有以 $p_i^{m_i}$ 为阶的元. 因此有阶为 $p_i^{t_i}$ 的元. 由(a)得证，这些元的积即所求以 c 为阶的元.

引理 2 Abel 群中如果有元 C 存在，其阶最大(在有限群中总有这种情况)，那么群的任何另一元 A 的阶 a 总是整除 c 的；所以群的每个元都满足 $x^c=1$.

证 如果 a 不是 c 的因子，那么 a 与 c 的最小公倍就大于 c，从而可以有此阶的元存在，这是与 c 的选出相矛盾的.

现在来证明命题 26. 设 S 的阶为 n，S 中元的最大阶为 r. 于是 S 所有元都满足 $x^r=1$. 这个 r 次多项式既然在体中不能多于 r 个根，由此得 $r\geqslant n$. 另一方面却有 $r\leqslant n$；因为每个元的阶总是 n 的因子. 所以 S 中有以 n 为阶的一个元 ε 存在，即 $1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{n-1}$ 这些元互异，从而表出了 S 的所有元. 于是 S 为循环群.

命题 26 也可以用(有限生成系的)Abel 群的基本命题来证明. 因为以后要用到这命题，就在这儿插进对它的一个证明.

设 G 为 Abel 群，其群运算写成加法. 设 G 中元 $g_1, g_2, \cdots, g_k$ 可以使 G 的每个元 g 表成 g_i 之倍的和，因此可写作形

如 $g=n_1g_1+\cdots+n_kg_k$，那么 $g_1, g_2, \cdots, g_k$ 就称为群 G 的生成元．如果小于 k 个元的系都不能生成 G，$g_1, g_2, \cdots, g_k$ 就称为一个最小的生成系．凡具有有限生成系的群还有最小生成系．尤其是有限群总有个最小生成系．

从恒同式 $n_1(g_1+mg_2)+(n_2-n_1m)g_2=n_1g_1+n_2g_2$ 得到：如果 $g_1, g_2, \cdots, g_k$ 生成群 G，那么 $g_1+mg_2, g_2, \cdots, g_k$ 也生成 G．

方程 $m_1g_1+m_2g_2+\cdots+m_kg_k=0$ 称为生成元间之一关系，$m_1, m_2, \cdots, m_k$ 为此关系的系数．

设 $G_1, G_2, \cdots, G_k$ 都是 Abel 群的子群，如果 G 中每个元 g 可唯一地表成和 $g=x_1+x_2+\cdots+x_k$，其中 x_i 是 G_i 之一元，$i=1,2,\cdots,k$，那么这 Abel 群 G 就称为这些子群 $G_1, G_2, \cdots, G_k$ 的**直积**．

基本命题 具有限生成元的 Abel 群是循环子群 $G_1, G_2, \cdots, G_k$ 的直积，其中 G_i 的阶是 G_{i+1} 的阶的因子，$i=1, \cdots, k-1$，并且 k 是一最小生成系的元数．此外，数 0 了解为其中无穷群的阶．

如果 $k=1$，那么群 G 是循环的，从而命题显然是对的．假设命题对于以 $k-1$ 个元为其最小生成系的所有群都是对的．设 G 为以 k 个元为其最小生成系的 Abel 群．如果根本没有最小生成系所满足的非平凡关系，那么设 $g_1, g_2, \cdots, g_k$ 为一最小生成系，从而 $G_1, G_2, \cdots, G_k$ 就是由这些元所生成的循环群．对于 G 中每个元 g 有唯一的表式 $g=n_1g_1+\cdots+n_kg_k$；否则就会得出一个非平凡关系了．如此情况命题为真．而今假设对于一个一定的最小生成系满足一个非平凡关系．这最小生成系满足的所有关系中有一关系

$$m_1g_1+\cdots+m_kg_k=0, \tag{1}$$

其中出现那最小的正系数．把这些生成元经过适当的编码，便可以假设那系数就是 m_1．在 $g_1, \cdots, g_k$ 另一任意的关系

$$n_1g_1+\cdots+n_kg_k=0 \tag{2}$$

中，m_1 必为 n_1 的因子．否则，$n_1=qm_1+r$，$0<r<m_1$，而且从关系(2)减去关系(1)的 q 倍就会引出系数 $r<m_1$ 的关系来了．关系(1)中的 m_1 还必定是 m_i 的因子；$i=2, \cdots, k$．否则，

$$m_2=qm_1+r,\ 0<r<m_1.$$

在生成系 $g_1+qg_2, g_2, \cdots, g_k$ 就有关系

$$m_1(g_1+qg_2)+rg_2+m_3g_3+\cdots+m_kg_k=0,$$

其中的系数 r 与所选 m_1 相矛盾．因此，

$$m_2=q_2m_1,\ m_3=q_3m_1,\ \cdots,\ m_k=q_km_1.$$

$$\bar{g}_1=g_1+q_2g_2+\cdots+q_kg_k,\ g_2,\ \cdots,\ g_k$$

这个系是最小生成系，并且 $m_1\bar{g}_1=0$．设

$$0=n_1\bar{g}_1+n_2g_2+\cdots+n_kg_k$$

是 $\bar{g}_1, g_2, \cdots, g_k$ 间的某一关系．把这关系看成关系(2)，$m_1\bar{g}_1=0$ 看成关系(1)，那么由于 m_1 整除 n_1，尤其是有 $n_1\bar{g}_1=0$ 这个关系．

设 G' 是由 $g_2, g_3, \cdots, g_k$ 生成的 G 的子群，G_1 是由 $\bar{g}_1$ 生成的阶为 m_1 的循环群．于是 G 就是 G_1 与 G' 的直积．其实，G 的每个元 g 可写成形式

$$g=n_1\bar{g}_1+n_2g_2+\cdots+n_kg_k=n_1\bar{g}_1+g',$$

其中 g' 属于 G'．这表示是唯一的；由于

$$n_1\bar{g}_1+g'=n_1'\bar{g}_1+g''$$

得到

$$(n_1-n_1')\bar{g}_1+(g'-g'')=0,$$

而刚才看到，从 $(n_1-n_1')\bar{g}_1=0$ 这样的一个关系因此就得到

$n_1\bar{g}_1=n_1'\bar{g}$. 把这个代入后自然也得到 $g'=g''$.

根据归纳假设，G' 是 $k-1$ 个循环群的直积，各由元 $\bar{g}_2$, $\bar{g}_3$, …, $\bar{g}_k$ 生成，按次序具有阶 t_2, …, t_k，对于 $i=2$, …, $k-1$，满足 t_i 是 t_{i+1} 的因子的条件. 考虑这些生成元 $\bar{g}_1$, $\bar{g}_2$, …, $\bar{g}_k$ 及关系 $m_1\bar{g}_1+t_2\bar{g}_2=0$，那么以前的论证就证明了 m_1 是 t_2 的因子. 这就完成了证明.

现在来讨论有限体，即具有有限个元的体.

设 K 为具 q 个元的有限体. K 中异于零的元作成 $q-1$ 阶的乘法群，从而 $\alpha^{q-1}=1$ 为体中元 $\alpha\neq 0$ 满足. 把这方程乘以 α，如此就得到 $\alpha^q=\alpha$，而今此方程对于 $\alpha=0$ 也成立. 根据命题 26，K 的乘法群是循环的，因此有一元 ε 使得其幂 1, ε, ε^2, …, ε^{q-2} 遍历 K 中异于零的元；ε 本身是阶为 $q-1$ 的元. 把这结论应用到 K 上的、具有有限次数的扩张 E，那就看到，E 的非零元都是一个单独的元 α 的幂，从而 $E=K(\alpha)$. 由此补足了命题 24 的证明所留下的缺陷.

现在设 $(E/K)=n$, ω_1, ω_2, …, ω_n 为 K 上的向量空间的生成元. E 的每个元 θ 有唯一的线性组合

$$\theta=c_1\omega_1+c_2\omega_2+\cdots+c_n\omega_n,$$

其中 c_i 属于体 K. 由此得到 E 中元数等于 q^n. 这 q^n 个元都满足 q^n 次方程 $x^{q^n}-x=0$. 因为这方程显然不会有多于 q^n 个根，E 中元正是这方程的所有根，从而每个根都是单根. 因此有分解

$$x^{q^n}-x=\prod_{\alpha}(x-\alpha),$$

积取遍 E 的所有元 α. 由此得到，E 就是 K 上的、多项式 $x^{q^n}-x$ 的分裂体. 由命题 10 的系得到，K 上的次数相同的任何两个扩张总是同构的，其中这种同构使 K 的每个元都不动.

因为 K 是有限体，这就保证它的特征不是 0．设 K 的特征为 $p>0$，那么 K 包含具有 p 个元的子体 Q_p．如果在 Q_p 上的 K 的次数为 r，那么由上所论，K 恰有 p^r 个元，即 $q=p^r$．已经发觉过在特征 p 的有限体中取 p 次幂是自同构．引用两次这种自同构，那么就看出取 p^2 次幂也是自同构．一般对于每个自然数 s，把 K 中每个 α 映成 α^{p^s} 的映射都是 K 的自同构．因此对于 K 中所有的 α，β，方程 $(\alpha\pm\beta)^{p^s}=\alpha^{p^s}\pm\beta^{p^s}$，$(\alpha\beta)^{p^s}=\alpha^{p^s}\beta^{p^s}$ 成立．

现在关于给定的具有 $q=p^r$ 个元的有限体 K 与给定的 $n\geqslant 1$ 还要证明次数为 n 的扩体 E 的存在．为此，设在 K 上的、多项式 $x^{p^n}-x$ 的分裂体为 E．要证的是 $(E/K)=n$．由前所论只须证明 E 的元数等于 q^n．设 α 为多项式的根，因此 $\alpha^{q^n}-\alpha=0$，于是也可以把多项式写成形如 $(x^{q^n}-\alpha^{q^n})-(x-\alpha)$．除以 $x-\alpha$ 并且以 $x=\alpha$ 代入，那么得到 $q^n\cdot\alpha^{q^n-1}-1$．因为特征整除 q，因此 q 当作体元是 0，刚才得到的就只是 -1．这就指明 α 是单根，于是 $x^{q^n}-x$ 正好有 q^n 个不同的根．同时 q^n 为 p 的幂，取 q^n 次幂就是一个自同构．如果 α 与 β 为方程的两个根，那么如下计算指出：$\alpha\pm\beta$，$\alpha\beta$ 以及 $\dfrac{\alpha}{\beta}(\beta\neq 0)$ 也都是方程的根：

$$(\alpha\pm\beta)^{q^n}=\alpha^{q^n}\pm\beta^{q^n}=\alpha\pm\beta,$$

$$(\alpha\beta)^{q^n}=\alpha^{q^n}\beta^{q^n}=\alpha\beta,$$

$$\left(\frac{\alpha}{\beta}\right)^{q^n}=\frac{\alpha^{q^n}}{\beta^{q^n}}=\frac{\alpha}{\beta}.$$

因此看出，方程的所有根本身作成具有 q^n 个元的体；并且由分裂体的最小性得到 E 就是这个体，于是具有 q^n 个元．

把上述应用到以 r 为扩张次数的 Q_p 基体，那就看到，对于给定的 $q=p^r$，有具 q 个元的体存在．由前所证明的这种扩

张的唯一性得到，具相等元数的两个有限体总是同构的．

设 K 为给定的具 q 个元的体，并设扩张次数为 n 的体为 E，那么就已经看到 E 可通过一个单独元的添加而生成．因此以 α 为根的 K 中不可约多项式是 n 次的．这就说明 K 中总有任给次数的不可约多项式．

现在要决定有限体 K 的 n 次扩张 E 的自同构群 G（即那些使 K 不动的自同构）．已经看到，对于 E 中所有的 α 使得 $\sigma(\alpha)=\alpha^q$ 的映射 σ 表示一个自同构．对于 E 中的 α 有 $\alpha^q=\alpha$，因此知道 σ 使 K 的每个元都不动．为了决定 σ 的阶，假定 $\sigma^s=1$．那就对 E 中所有的 α 需要 $\alpha^{q^s}=\alpha$．因为，当 $s\geqslant n$ 时多项式 $x^{q^s}-x$ 只能有 q^n 个根，另一方面，又因为 $\alpha^{q^n}=\alpha$ 对于 E 中所有的 α 都满足，σ 的阶就是 n．而今就得到 n 个不同的自同构 $1, \sigma, \sigma^2, \cdots, \sigma^{n-1}$．$n$ 次扩张不可以有更多的自同构．因此就决定了 G，并且接着指明它为 n 阶的循环群．

K．单 位 根

如果 K 为任一体，ε 为其一扩体中元且是 x^n-1 的根，那么 ε 称为 n 次**单位根**．

如果 K 的特征 p 是大于 0 的，并且 $n=pm$，那么 $x^n-1=(x^m-1)^p$，因此每个 n 次单位根就已经是 m 次的了．因此，假设特征 $p>0$，因为这对一般性并无限制，还设 n 与 p 是互素的．

x^n-1 的导数为 nx^{n-1}，它只有根 0，因此与 x^n-1 无公根．K 上的、x^n-1 的分裂体 E 于是为正规扩张，并且正好含有 x^n-1 的 n 个根．因为两个单位根的积与商仍为单位根，所以这些 n 次单位根在 E 中作成乘法群．因此根据命题

26，它作成循环群．于是有一个阶恰为 n 的 n 次单位根 ε．所有 n 次单位根都是 ε 的幂．这种单位根 ε 称为 n 次原根．如果 i 与 n 互素，那么幂 ε^i 就正好是个 n 次原根．因此，不同的 n 次原根的个数由 Euler 函数 $\varphi(n)$ 给出，这函数想必在数论初步中已是熟悉的了．

如果 d 为 n 的因子，那么 x^d-1 就是 x^n-1 的因子．因此这些 d 次单位根全部在 n 次单位根中出现．任一幂 ε^i 就以 n 的因子 d 作为其阶，并且它就是 d 次原根．如果用 $\Phi_d(x)$ 来记多项式 $\prod(x-\eta)$，其中 η 取遍所有的 d 次原根，那么就得到

$$(*)\qquad x^n-1=\prod_d \Phi_d(x),$$

其中 d 遍历 n 的一切因子；这正是因为此式右方只不过把左方出现的单位根按阶 d 进行汇集．$\Phi_1(x)=x-1$，通过对 n 作归纳法来证明 $\Phi_n(x)$ 为整系数多项式．由归纳假设从(*)得

$$x^n-1=\Phi_n(x)g(x),$$

其中 $g(x)$ 为以 1 为最高系数的整系数多项式．因此由除法得出 $\Phi_n(x)$ 也是以 1 为最高系数的整系数多项式．这个多项式 $\Phi_n(x)$ 有次数 $\varphi(n)$，并且称之为 n 次**分圆多项式**．式(*)在任一体中表明 x^n-1 的一个有用的分解；那些因子一般却不是不可约的．

如果 ε 为 n 次原根，那么 $K(\varepsilon)$ 这体已包含所有的 n 次单位根，因此就是 x^n-1 的分裂体 E．因为 $\Phi_n(\varepsilon)=0$，就有 $(E/K)\leqslant\varphi(n)$．设 G 为关于 K 的 E 的自同构群并且 σ 为 G 的元．因为 n 次原根由自同构作出的象仍为 n 次原根，$\sigma(\varepsilon)=\varepsilon^i$ 中的 i 必与 n 互素．此时 $\sigma(\varepsilon^j)=\varepsilon^{ij}=(\varepsilon^j)^i$，因此 σ 把每个 n 次单位根代以其 i 幂．这就说明数 i 只与 σ 相关，

而与 n 次原根 ε 的选择无关，当然其中的 i 只是除去 n 的倍数来决定的．而且不一定每个与 n 互素的 i 就产生一个自同构．例如 ε 属于 K 本身，于是 $E=K$，σ 必为恒同映射，因此只有 $i\equiv 1(\mathrm{mod}\, n)$．

现在如果把与 i 相关的 σ 记为 σ_i，那么就有 $\sigma_i\sigma_j(\varepsilon)=\sigma_i(\varepsilon^j)=\varepsilon^{ij}$，于是 $\sigma_i\sigma_j=\sigma_{ij}$．对于每个 σ_i，有唯一的一个与 n 互素的模 n 同余类对应，而两个自同构的积与彼此相应的同余类之积对应．因此，群 G 与 n 互素的模 n 同余类群的子群同构，特别由 $\sigma_i\sigma_j=\sigma_{ij}=\sigma_j\sigma_i$ 看到，G 还是个 Abel 群．

只对特殊的体 K 才能推测更精确的命题．这方面最重要的结果是

命题 27 对于 $K=Q$ 这个有理数体，多项式 $\Phi_n(x)$ 是不可约的，因此 $(E/Q)=\varphi(n)$．由任意与 n 互素的 i 产生的映射 $\sigma_i(\varepsilon)=\varepsilon^i$ 为 G 中自同构，并且 G 同构于所有与 n 互素的同余类的乘法群．如果 n 是一素数 p，那么 G 这个群是阶为 $p-1$ 的循环群，并且

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1.$$

证 设多项式 $f(x)$ 是 x^n-1 的因子而且其系数都是有理数．乘以适当常数后可假定 $f(x)$ 具有整系数．（如果使用论整系数多项式的 Gauss 命题，那就还可以假设这 $f(x)$ 有 1 为最高系数；然而这里用不着这个）．设 s 为自然数，$r_s(x)$ 为 $f(x^s)$ 除以 $f(x)$ 所得余式，于是 $r_s(x)$ 具有理系数，并且这些系数的分母中只出现那些能整除 $f(x)$ 最高系数的素因子．如果把形如 $f(x)g(x)$ 的多项式与 $f(x^s)$ 相加，那么除以 $f(x)$ 所得余式不变．设 ax^m 为 $f(x)$ 之一项，那么此项在差 $f(x^{s+n})-f(x^s)$ 中便产生项 $ax^{m(s+n)}-ax^{ms}=ax^{ms}(x^{mn}-1)$，这是可被 x^n-1 整除的，因此可被 $f(x)$ 整除．这就指出 $r_{s+n}(x)=r_s(x)$，

所以 $r_s(x)$ 就只与模 n 的 s 所属同余类有关．尤其是只存在有限个不同的多项式 $r_s(x)$．

现在设 p 为素数；它不能整除 $f(x)$ 的最高系数．多项式 $r_p(x)$ 也是多项式 $f(x^p)-(f(x))^p$ 的除法余式．因为 $f(x)$ 具整系数，就有形式 $f(x)=\sum\pm x^m$，其中每个单独的项可出现多次．由于以前论述的二项式系数的那种可除性，$(f(x))^p$ 与 $\sum\pm x^{mp}$ 只差一个具有可被 p 整除的整系数多项式．因为 $f(x^p)=\sum\pm x^{pm}$，故得 $f(x^p)-(f(x))^p=pg(x)$；$g(x)$ 为整系数多项式．因此 $r_p(x)$ 是 $g(x)$ 的除法余式的 p 倍，又因为 p 不能整除 $f(x)$ 的最高系数，所以 p 就整除 $r_p(x)$ 每个系数的分子．

今设 M 为整数，它超过 $f(x)$ 的最高系数而且大于所有多项式 $r_s(x)$ 所有系数的分子（已知只有有限个不同的 $r_s(x)$）．如果 p 为 $\geqslant M$ 的素数，那么只有 $r_p(x)=0$，p 才除得尽 $r_p(x)$ 每个系数的分子．因此知道，对于所有 $\geqslant M$ 的素数 p 总有 $r_p(x)=0$．

现在设 s 与 t 是使得

$$r_s(x)=0 \text{ 与 } r_t(x)=0$$

的整数．这就是说 $f(x^s)$ 可被 $f(x)$ 整除，从而 $f(x^{st})$ 可被 $f(x^t)$ 整除．又因为 $f(x^t)$ 可被 $f(x)$ 整除，得 $r_{st}(x)=0$．因此，只要 s 的所有素因子大于或等于 M，就有 $r_s(x)=0$．

这时来设 s 为任一与 n 互素的数．取 $s_1=s+n\prod p$，其中 p 取遍那些小于 M 的素数而又除不尽 s 的．读者容易证实 s_1 不能被低于 M 的素数整除，因此 $r_{s_1}(x)=0$．因为 s 与 s_1 属于模 n 的同一同余类，所以 $r_s(x)=0$．由此证明了，如果 s 与 n 互素，那么 $f(x^s)$ 可被 $f(x)$ 整除．

此外，还假设 $f(x)$ 有原根 ε 为其零点．如果 s 与 n 互

素，那么 $f(x^s)=f(x)h(x)$，因此也有 $f(\varepsilon^s)=0$. 所以一切 n 次原根都是 $f(x)$ 的零点，从而 $f(x)$ 的次数 $\geqslant\varphi(n)$. 因为分圆多项式 $\Phi_n(x)$ 的次数正好是 $\varphi(n)$，因此它必为不可约的. 同时群 G 必须正好含有 $\varphi(n)$ 个元，对于任一与 n 互素的 i, σ_i 就产生一个自同构.

如果 n 是素数 p，那么群 G 同构于模 p 的与 p 互素的那些同余类作成的乘法群. 然而它就是体 Q_p 的乘法群，从而是循环群. 由 $x^p-1=\Phi_p(x)\Phi_1(x)$ 得到 Φ_p 那申明的值.

因此证明了命题 27 的一切.

L. Noether 方程

设 E 为体而 G 为 E 的有限自同构群. 设对应于 G 中的每个元 σ，都有 E 中一元 $x_\sigma\neq 0$，还假设此元满足下列方程：

$$x_\sigma\cdot\sigma(x_\tau)=x_{\sigma\tau},$$

对于 G 中所有的 σ 与 τ 都成立. 于是把 x_σ 称为这个 **Noether 方程**的解.

命题 28 对于所有的 σ，Noether 方程具有 $x_\sigma=\dfrac{\alpha}{\sigma(\alpha)}$ 这种唯一类型的解，其中 α 是 E 中异于零的、一个固定的但是可任意选择的元.

证 对于任意元 α，显然 $x_\sigma=\dfrac{\alpha}{\sigma(\alpha)}$ 就是方程的解，正是由于

$$\frac{\alpha}{\sigma(\alpha)}\cdot\sigma\left(\frac{\alpha}{\tau(\alpha)}\right)=\frac{\alpha}{\sigma(\alpha)}\cdot\frac{\sigma(\alpha)}{\sigma\tau(\alpha)}=\frac{\alpha}{\sigma\tau(\alpha)}.$$

反之，设 x_σ 是方程的一解. 因为这些自同构是线性无关的，方程 $\sum\limits_\tau x_\tau\tau(z)=0$（把所有的 τ 加起来）就不能对于 E 中所有的 z 都成立. 于是 E 中有一元 a 使得 $\sum\limits_\tau x_\tau\tau(a)=\alpha\neq 0$.

把 σ 作用于 α, 就得到

$$\sigma(\alpha)=\sum_{\tau}\sigma(x_{\tau})\cdot\sigma\tau(a).$$

乘以 x_{σ}, 得

$$x_{\sigma}\cdot\sigma(\alpha)=\sum_{\tau}x_{\sigma}\sigma(x_{\tau})\cdot\sigma\tau(a).$$

以 $x_{\sigma\tau}$ 代 $x_{\sigma}\cdot\sigma(x_{\tau})$ 并注意 $\sigma\tau$ 因 τ 而取遍群 G 的元, 因此得到

$$x_{\sigma}\cdot\sigma(\alpha)=\sum_{\tau}x_{\tau}\tau(a)=\alpha,$$

所以

$$x_{\sigma}=\frac{\alpha}{\sigma(\alpha)}$$

是正确的.

设 K 为 G 的不动点体. 如果只考虑 Noether 方程那些在 K 中的解, 那么方程便简化为

$$x_{\sigma\tau}=x_{\sigma}x_{\tau},$$

正是因为 σ 使 K 的元不动. 如果把 x_{σ} 看成从 G 到 K 的映射, 那么这方程表明 x_{σ} 是个从 G 到 K 的特征标. 把这和命题 28 结合起来, 就得到

命题 29 设 E 是具有群 G 的、K 上的正规扩张. 对应于 G 到 K 中的每个特征标 $C(\sigma)$, 可以在 E 中找到一个元 $\alpha\neq 0$, 使得 $C(\sigma)=\frac{\alpha}{\sigma(\alpha)}$. 反之, 如果 $\alpha\neq 0$ 是 E 中一元, 它使得对于所有的 σ 都有 $C(\sigma)=\frac{\alpha}{\sigma(\alpha)}$ 在 K 之中, 那么 $C(\sigma)$ 是从 G 到 K 的特征标. 于是, 这个元 α 具有 α^{r} 属于 K 的性质; 其中 r 是 G 的群元那些阶的最小公倍.

命题 29 最后一段之前的部分都已证明过了. 为了证明最后一段, 只要证明对于 G 的每个 σ, $\sigma(\alpha^{r})=\alpha^{r}$ 都成立. 然而这就是

$$\frac{\alpha^r}{\sigma(\alpha^r)}=\left(\frac{\alpha}{\sigma(\alpha)}\right)^r=(C(\sigma))^r=C(\sigma^r)=C(1)=1.$$

还提出命题 28 的一个应用. E 中元 α 经 G 中所有自同构作用所得象的积是 K 的元; 因为显然这积是属于 G 的不动点体的. 把它称为 α 的范数并记作 $N(\alpha)$. 显然有

$$N(\alpha)N(\beta)=N(\alpha\beta),$$

$$N\left(\frac{\alpha}{\beta}\right)=\frac{N(\alpha)}{N(\beta)}.$$

如果 σ 属于 G, 那么在 G 的所有元作用下 $\sigma(\alpha)$ 的那些象就和 α 的相同, 因此 $N(\alpha)=N(\sigma(\alpha))$. 对于 $\alpha\neq 0$, 就有 $N\left(\frac{\alpha}{\sigma(\alpha)}\right)=1$. 在以循环群为自同构群的体中, 逆命题是正确的, 这应归功于 Hilbert.

命题 30 如果 K 上的正规扩张 E 的群 G 是以 σ 为生成元的 n 阶循环群, 那么用 E 中元 $\alpha\neq 0$ 作出的元 $\beta=\frac{\alpha}{\sigma(\alpha)}$, 就是方程 $N(\beta)=1$ 的唯一的解.

证 群 G 由这些元 σ^i 组成, 其中的 i 取一切正整数. 设

$$N(\beta)=\prod_{\nu=0}^{n-1}\sigma^\nu(\beta)=1.$$

对每个 i 取

$$x_{\sigma^i}=\prod_{\nu=0}^{i-1}\sigma^\nu(\beta).$$

因此 x_{σ^i} 其实只与 σ^i 相关. 得到

$$x_{\sigma^i}\sigma^i(x_{\sigma^k})=\prod_{\nu=0}^{i-1}\sigma^\nu(\beta)\prod_{\mu=0}^{k-1}\sigma^{i+\mu}(\beta)=\prod_{\nu=0}^{i+k-1}\sigma^\nu(\beta)=x_{\sigma^{i+k}}.$$

这组 x_{σ^i} 因此就是 Noether 方程的解, 从而由命题 28, E 中有

元 $\alpha\neq0$ 存在，使得 $x_{\sigma^i}=\dfrac{\alpha}{\sigma^i(\alpha)}$. 于是，对于 $i=1$，一方面得到 $x_\sigma=\beta$，另一方面 $x_\sigma=\dfrac{\alpha}{\sigma(\alpha)}$. 由此证明了命题.

M. Kummer 体

设 K 为含 r 次原根的体，G 为具指数 r 的有限 Abel 乘法群，即每个元的阶都是 r 的因子的 Abel 群. G 到 K 的特征标以后简称 G 的**特征标**. 对于每个特征标 $C(\sigma)$，总有 $(C(\sigma))^r=C(\sigma^r)=C(1)=1$，因此看出这些特征标的值是 r 次单位根. 如果 C_1 与 C_2 为特征标，那么 $C_1(\sigma)C_2(\sigma)$ 也是特征标，把它记作 C_1C_2. 因为 $(C(\sigma))^{-1}$ 也是特征标，这些特征标按如此合成就作成群 $\hat{G}$——**特征标群**或 G **的对偶群**.

如果把 Abel 群的基本命题摹述成对于乘法群的，那么就看出，群 G 中有 k 个元 τ_1, τ_2, $\cdots$, τ_k，其阶分别为 m_1, m_2, $\cdots$, m_k，使得 G 的每个元 σ 都可写成形式

$$(*)\qquad \sigma=\tau_1^{i_1}\tau_2^{i_2}\cdots\tau_k^{i_k}.$$

而且 i_ν 由模 m_ν 唯一决定.

如果 C 为特征标，并且 $\varepsilon_\nu=C(\tau_\nu)$（为 m_ν 次单位根，由于 m_ν 是 τ_ν 的阶），那么 $C(\sigma)=\varepsilon_1^{i_1}\varepsilon_2^{i_2}\cdots\varepsilon_k^{i_k}$. 反之，如果把每个 ε_ν 选成 m_ν 次单位根，那么上式就定义了 G 的特征标. 因此，每个特征标可以描写成向量 $(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k)$，并且与两个特征标之积相应的就是相应的两个向量按分量次序作积得到的向量. 设 C_s 是这样的特征标：描写它的向量中分量 ε_s 为 m_s 次原根而其它的 ε_ν 为 1. 于是显见每个特征标 C 可写成形式 $C=C_1^{l_1}C_2^{l_2}\cdots C_k^{l_k}$，其中 l_ν 由模 m_ν 唯一决定. 这就指出群 G 与群 $\hat{G}$ 是同构的，尤其是与 G 同阶. 如果把 G 中给定的元

$\sigma \neq 1$ 写成形式(*)，那么就有个指数 m_ν 整除 i_ν. 于是与它相关的 $C_\nu(\sigma) \neq 1$. 因此，对于每个元 $\sigma \neq 1$, 总可以找到特征标 C, 使得 $C(\sigma) \neq 1$.

设 σ 为 G 的元. 以特征标 C 作为变量把元 $C(\sigma)$ 看成 C 的函数. 因为特征标的积 C_1C_2 已由式 $C_1C_2(\sigma) = C_1(\sigma)C_2(\sigma)$ 说明，这个 C 的函数就是 $\hat{G}$ 的特征标. 因此，对于 G 的每个元 σ, 就有 $\hat{G}$ 的一个特征标与它对应. $\hat{G}$ 的两个这样的特征标 $C(\sigma)$ 与 $C(\tau)$ 之积应当由 $C(\sigma)C(\tau) = C(\sigma\tau)$ 来说明，从而看到元 $C(\sigma\tau)$ 对应于此积. 如果 $\sigma \neq \tau$, 两个特征标 $C(\sigma)$ 与 $C(\tau)$ 可以一致吗?就是说，对于所有的 C 会不会总是 $C(\sigma) = C(\tau)$, 也就是 $C(\sigma\tau^{-1}) = 1$. 但是，因为 $\sigma\tau^{-1} \neq 1$就总有个 C 使得 $C(\sigma\tau^{-1}) \neq 1$. 既然 $\hat{G}$ 的特征标群与 $\hat{G}$ 等阶，因此与 G 等阶，如果 σ 取遍 G 所有元，那么 $C(\sigma)$ 生成 $\hat{G}$ 的所有特征标. 所以自然可以把 G 看成 $\hat{G}$ 的特征标群.

目前要把节 L 中所证明的命题应用到一定的体扩张上. 设 K 为含 r 次原根的体，并且 E 为 K 的正规扩张，它的自同构群 G 为具指数 r 的 Abel 群. 此中将要证明这体 E 是可以通过 K 中元的 r 次根的添加而得到. 因此提示，考虑 E 中作为 K 的元的 r 次根的元 $\alpha \neq 0$ 组成的集 A, 因此就是那些 α^r 属于 K 的 α 所成集. 集 A 为乘法群而且显然包含 K 所有非零元集 K^* 作为其子群. 商群 A/K^* 与 G 的特征标群 $\hat{G}$ 有密切联系. 就是说，如果 C 为 G 的特征标，那么由命题 29, 就有 E 的元 $\alpha \neq 0$ 使得 $C(\sigma) = \dfrac{\alpha}{\sigma(\alpha)}$ 对每个 σ 都成立；并且 α^r 属于 K, 因此 α 就是 A 的元. 如果 $\dfrac{\alpha}{\sigma(\alpha)} = \dfrac{\beta}{\sigma(\beta)}$ 对一切 σ 都成立，那么 $\dfrac{\alpha}{\beta} = \sigma\left(\dfrac{\alpha}{\beta}\right)$, 所以 $\dfrac{\alpha}{\beta}$ 必在K^*中. 因此

正好有一个旁系 αK^* 对应于特征标 C. 反之，如果 α 为 A 的元，那么 $\alpha^r=a$ 是 K^* 的元，因此 $(\sigma(\alpha))^r=a$, 所以 $\frac{\alpha}{\sigma(\alpha)}$ 是 r 次单位根，它就是 K^* 的元. 于是根据命题 29, $\frac{\alpha}{\sigma(\alpha)}$ 是 G 的特征标. 因此这种对应给出映 $\hat{G}$ 成商群 A/K^* 的一一映射. 如果

$$C_1(\sigma)=\frac{\alpha}{\sigma(\alpha)},\ C_2(\sigma)=\frac{\beta}{\sigma(\beta)},$$

那么

$$C_1C_2(\sigma)=\frac{\alpha\beta}{\sigma(\alpha\beta)}.$$

这就指出映射是把 $\hat{G}$ 映成 A/K^* 的同构. 尤其是 A/K^* 为有限群. 现在把 A 的所有元添加于 K 并且记所得中间体为 E_0, E_0 所属的 G 的子群记作 U, 它就使得 E_0 所有元都不动. U 尤其使 A 的元不动. 如果 U 含有元 $\sigma\neq1$, 既然 G 为 Abel 群，那么可以找到一个特征标 C 使得 $C(\sigma)\neq1$. 由于 A 中有适当的 α 使 $C(\sigma)=\frac{\alpha}{\sigma(\alpha)}$, 因此 σ 就使这 α 不是不动的了，此为矛盾. 而今由 $U=1$ 便得到 $E_0=E$.

K 与 E 之间的每个体 E_1 属于 G 的一个子群 U. 因为 G 是 Abel 的，U 即为 G 的正规子群，因此 E_1 为 K 的正规扩张，其自同构群 G/U 仍为具指数 r 的 Abel 群. 于是发展过的理论就可以应用在 E_1 上. E_1 是由 K 通过集 B 的添加于 K 得到的；而且 B 由 E_1 中那些使得 β^r 处于 K 中的元 $\beta\neq0$ 组成的集. 显然 B 是含有 K^* 的、为 A 所包含的子群. 所以 K^* 与 A 之间的中间群至少如中间体 E_1, 即 G 的子群 U 一样多. 但是任一中间群 B 正好有 A/K^* 的一个子群 B/K^* 与

它对应．A/K^* 与 $\hat{G}$ 同构，因此与 G 同构．这就指出中间群的个数一如子群 U 的个数．于是建立了映中间体 E_1 为中间群 B 的一一映射．尤其是通过异于 A 的中间群的添加所得绝不会是整个的体 E.

以 A^r 记 A 中所有元 r 次幂的集，K^{*r} 记 K^* 中所有元 r 次幂的集，它们的 r 次根都在 E 中，商群 A^r/K^{*r} 由旁系 aK^{*r} 组成，并且 aK^{*r} 的元的 r 次根与 $\sqrt[r]{a}$ 的区别只不过是 K^* 中平凡的因子．读者容易证实，由旁系 αK^* 对应旁系 $\alpha^r K^{*r}$ 把 A/K^* 映成 A^r/K^{*r} 的映射表示同构．由此，凭借基体的元可描写特征标群 $\hat{G}$.

如果还假设 G 又是循环的．于是 A/K^* 也是循环的，因此由一个单独旁系 αK^* 的幂组成．只需通过这个单独元 α 添加于 K 就足以代替把 A 添加于 K．如此情况，E 就由 K 通过添加 K 的元的一个单独的 r 次根而生成．

把至今所得的结果总结为

命题 31 设 K 为含 r 次原根的体，E 为 K 的正规扩张，其自同构群 G 为具指数 r 的 Abel 群．这样的扩张称为 **Kummer 体**．如果 A 为 E 中使得 α^r 属于 K 的元 $\alpha\neq 0$ 所成集，那么 $\hat{G}$ 与 A/K^* 而且与 A^r/K^{*r} 同构．E 由 K 通过添加集 A 而生成．如果 B 是 A 与 K^* 之间的群，那么 $K(B)$ 是中间体，并且这些 B 与这些中间体有一一对应的关系．如果 G 是循环的，那么 E 可以由 K 通过添加 K 中一元的一个单独的 r 次根而生成．

如果 $a_1, a_2, \cdots, a_t$ 是在 K 中给定的异于零的元，那么把记法 $E=K(\sqrt[r]{a_1}, \sqrt[r]{a_2}, \cdots, \sqrt[r]{a_t})$ 了解为多项式 $(x^r-a_1)\cdot(x^r-a_2)\cdots(x^r-a_t)$ 的分裂体（正是因为因子 x^r-a 的不同各根彼此区别只在于单位根，而这些单位根又是属于 K 的）．

多项式 x^r-a_ν 的导数是 rx^{r-1}，并且只有根 0，这是因为 r 不能被 K 的特征整除，当 r 次原根属于 K 时．因此，每个因子 x^r-a_ν 只有单根，于是 E 就是 K 的正规扩张．记法 $\sqrt[r]{a_\nu}$ 是作为 x^r-a_ν 的某个选定的根 α_ν 来了解的．E 的自同构 σ 只不过使 α_ν 取得单位根 $\varepsilon_\nu(\sigma)$ 为其因子；因为由 $\alpha_\nu^r=a_\nu$ 得 $(\sigma(\alpha_\nu))^r=a_\nu$．因此 $\sigma(\alpha_\nu)=\varepsilon_\nu(\sigma)\alpha_\nu, \nu=1, 2, \cdots, t$，并且因为这些 α_ν 生成体 E，σ 就由这些式子来描写．如果 σ 与 τ 是 E 的自同构群的元，那么得到

$$\tau(\sigma(\alpha_\nu))=\varepsilon_\nu(\sigma)\tau(\alpha_\nu)=\varepsilon_\nu(\sigma)\varepsilon_\nu(\tau)\alpha_\nu,$$

因为 $\varepsilon_\nu(\sigma)$ 是在 K 中的．另一方面，$\tau(\sigma(\alpha_\nu))=\varepsilon_\nu(\tau\sigma)\alpha_\nu$，从而 $\varepsilon_\nu(\tau\sigma)=\varepsilon_\nu(\sigma)\cdot\varepsilon_\nu(\tau)$．由此得 $\varepsilon_\nu(\tau\sigma)=\varepsilon_\nu(\sigma\tau)$，所以 G 是 Abel 群．还有 $\varepsilon_\nu(\sigma^r)=(\varepsilon_\nu(\sigma))^r=1$，因此 G 具有指数 r．

如果 $t=1$，于是 $E=K(\sqrt[r]{a_1})$，那么只有一个单独的 $\varepsilon_1(\sigma)$ 出现，于是 G 同构于随着出现的那些单位根构成的群．作为体的有限乘法群它是循环的，并且作为 r 次单位根所成群的子群，其阶为 r 的因子．

如果仍回到任意的 t，还考虑具形如 $\alpha_1^{\nu_1}\cdot\alpha_2^{\nu_2}\cdots\alpha_t^{\nu_t}\cdot a$ 的所有元作成的乘法群，其中 ν_i 为任意整数，a 为 K^* 的任一元．这群是 A 的子群并且包含 K^*．当把它添加于 K，它就生成 E 这个体．所以它必定就是 E 中整个的群 A．

群 A^r 由形如 $a_1^{\nu_1}\cdot a_2^{\nu_2}\cdots a_t^{\nu_t}\cdot a^r$ 的元组成，其中 ν_i 为任意整数，a 为 K^* 中任意元，于是群 $\hat{G}$ 与商群 A^r/K^{*r} 同构．

于是得到

命题 32 如果 K 为含 r 次原根的体，$a_1, a_2, \cdots, a_t$ 为 K^* 中任意的元．那么扩张 $E=K(\sqrt[r]{a_1}, \sqrt[r]{a_2}, \cdots, \sqrt[r]{a_t})$ 就是 Kummer 体．它的自同构群的特征标群 $\hat{G}$ 同构于

A^r/K^{*r}，其中 A^r 是形如 $a_1^{\nu_1}\cdot a_2^{\nu_2}\cdots a_t^{\nu_t}\cdot a^r$ 的具整数 ν_i 与 K^* 中任意元 a 的所有元的集.

对于 $t=1$，自同构群是循环的，并且其阶是 r 的因子.

N. 正规基的存在

下列命题对任何体都成立，然而此处只证明对于 K 含有无穷多个元的情形.

命题 33 如果 E 为 K 的正规扩张，$\sigma_1, \sigma_2, \cdots, \sigma_n$ 是它的自同构群 G 的元，那么 E 中有这样的元 θ 存在，使得 n 个元 $\sigma_1(\theta), \sigma_2(\theta), \cdots, \sigma_n(\theta)$ 关于 K 是线性无关的.

证 根据命题24的系，有一这样的 α 存在，使得 $E=K(\alpha)$. 设 $f(x)$ 是 α 的不可约多项式. 取 $\sigma_i(\alpha)=\alpha_i$,

$$g(x)=\frac{f(x)}{(x-\alpha)f'(\alpha)},$$

而且

$$g_i(x)=\sigma_i(g(x))=\frac{f(x)}{(x-\alpha_i)f'(\alpha_i)}.$$

$g_i(x)$ 是 E 中的多项式，对于 $k\neq i$，有 α_k 为其根，所以对于 $i\neq k$，有

$$g_i(x)g_k(x)\equiv 0(\operatorname{mod} f(x)). \tag{1}$$

方程

$$g_1(x)+g_2(x)+\cdots+g_n(x)-1=0, \tag{2}$$

左方的次数最高为 $n-1$. 如果(2)对于 x 的 n 个不同值成立，那么左方必恒等于0. 这样的 n 个值就是 $\alpha_1, \alpha_2, \cdots, \alpha_n$，因为 $g_i(\alpha_i)=1$，并且对于 $k\neq i$，有 $g_k(\alpha_i)=0$.

以 $g_i(x)$ 乘(2)，引用(1)就得到

$$(g_i(x))^2\equiv g_i(x)(\operatorname{mod} f(x)). \tag{3}$$

现在来证行列式

$$D(x)=|\sigma_i\sigma_k(g(x))|, \quad i, k=1, 2, \cdots, n, \tag{4}$$

是异于零的．按列与列相乘求其平方$(\bmod f(x))$．由(1)，(2)与(3)求得主对角线元为1，其余位置都是零．因此

$$(D(x))^2\equiv 1(\bmod f(x)),$$

所以尤其有 $D(x)\neq 0$.

方程(4)右方的变量 x 是作为经所有自同构而不动来对待的．所以(4)中的 x 可代以特殊值，只要这些值经所有自同构也是不动的，即可以 K 中元来代入．

$D(x)$在 K 中只可能有有限个根．如果在 K 中选出 a 异于这些根，就有 $D(a)\neq 0$．取 $\theta=g(a)$．于是行列式

$$|\sigma_i\sigma_k(\theta)|\neq 0. \tag{5}$$

现在考虑任一线性关系 $x_1\sigma_1(\theta)+x_2\sigma_2(\theta)+\cdots+x_n\sigma_n(\theta)=0$，其中 x_i 取自 K．所有的自同构 σ_i 作用于它就得到 n 个未知量 x_i 的 n 个齐次方程，并以(5)为其行列式．因此所有的 $x_i=0$，从而证明了命题．

凭借这样的元 θ 通过 G 得出的象生成**正规基**，尤为简单的是可以算出属于 G 的子群 U 的中间体．E 的每个元 α 可写成唯一的式

$$\alpha=\sum_{\sigma} c_\sigma\sigma(\theta), \tag{6}$$

其中 σ 取遍 G 而 c_σ 为 K 中的元．α 作为 U 的不动点体的元，当且仅当对 U 所有的 τ 有 $\tau(\alpha)=\alpha$．如果用 τ 作用于(6)，把对 σ 求和代以对 $\tau^{-1}\sigma$ 的，那么得到

$$\tau(\alpha)=\sum_{\sigma} c_{\tau^{-1}\sigma}\sigma(\theta).$$

当 $c_{\tau^{-1}\sigma}=c_\sigma$ 对 U 所有的 τ 与 G 所有的 σ 都成立时，元 α 正好就是不动体中的元．$\tau^{-1}\sigma$ 因固定 σ 而遍历旁系 $U\sigma$．所得的条件就是说，c_σ 在整个旁系上取相同的值．把旁系 $U\sigma$ 所有

自同构作用于θ所得象的和记为$U\sigma(\theta)$. 因此, 如果$U\sigma_1$, $U\sigma_2$, $\cdots$, $U\sigma_j$是所有的旁系, 那么属于U的不动点体就由形如

$$\alpha=c_1U\sigma_1(\theta)+c_2U\sigma_2(\theta)+\cdots+c_jU\sigma_j(\theta)$$

的所有元组成, 其中c_j属于K. 因此j个元$U\sigma_i(\theta)$就生成属于U的不动点体这个K上的向量空间.

如果U是G的正规子群, 那么$U\sigma_i=\sigma_iU$, 从而得到$U\sigma_i(\theta)=\sigma_i(U(\theta))$. 这就指示$U(\theta)$产生不动点体的正规基.

O. 平移命题

设$p(x)$是体K中的可分多项式, E是$p(x)$的分裂体. 还设B是K的任一扩张. 如果把$p(x)$看成B中的多项式, 就用EB来记$p(x)$的分裂体. 因此, 如果α_1, α_2, $\cdots$, α_s是$p(x)$在EB里的根, 那么$K(\alpha_1, \alpha_2, \cdots, \alpha_s)$是$EB$的子体, 自然是$p(x)$在$K$上的分裂体. 根据命题10的系, E与$K(\alpha_1, \alpha_2, \cdots, \alpha_s)$是同构的. 所以, 取$E=K(\alpha_1, \alpha_2, \cdots, \alpha_s)$并不失其一般性, 从而假设$E$是$EB$的子体. 而且$EB=B(\alpha_1, \alpha_2, \cdots, \alpha_s)$. EB就是既含E又含B的最小体. 把它称为由E与B合成的体, 并且这就说明了记法EB.

用$E\cap B$来记既在E中又在B中的那些元的集. 容易看出, $E\cap B$是体, 并且是K与E间的中间体.

命题34(平移命题) 如果G是K上的E的自同构群, H是B上的EB的自同构群, 那么H同构于G的那个以$E\cap B$为不动点体的子群.

证 设σ是H的元. 它使体B不变, 从而也使体K不变. 随着是映体E到EB的同构, 并且根据命题17, 此映射由G之一元$\bar{\sigma}$来实现, 因此$\bar{\sigma}$是唯一的. 如果已知$\bar{\sigma}$, 那么

就知道 E 的生成元 α_i 的 $\bar{\sigma}$ 象；并且因为 α_i 也是 B 上的 EB 的生成元，这就得出了 σ. 因此这种对应是个从 H 到 G 的一一映射. H 中两元之积 $\sigma\tau$ 对应于 $\overline{\sigma\tau}$ 是显然的. 于是存在从 H 到 G 的同构.

接着为了描述 H，可以探问象群 $\bar{H}$ 的性质，尤其是 $\bar{H}$ 的不动点体. 它是 E 中那些在 $\bar{H}$ 的每个元 $\bar{\sigma}$、也就是在 H 的每个元 σ 作用下不动的元 α 组成的. 因为 B 是 H 的整个不动点体，所以 $\bar{H}$ 的不动点体就是 $E\cap B$ 这个体.

III

应　用

A. N. Milgram

A. 要用到的群论中的某些命题

设 M 与 M' 为集. 如果 f 是从 M 到 M' 的映射, A 是 M 的子集, 那么用 $f(A)$ 来记 A 的所有元 a 的象 $f(a)$ 组成的集; $f(A)$ 称为 A 的象. 如果 B 是 M' 的子集, 就用 $f^{-1}(B)$ 来记 M 中所有那些 $f(m)$ 属于 B 的元 m 组成的集; $f^{-1}(B)$ 称为 B 的原象. 因为 f 不一定是映 M 成 M' 的映射, 可能也出现那样的非空集 B 使得 $f^{-1}(B)$ 是空集. 已经介绍过用 $A_1 \cap A_2$ 来记集 A_1 与集 A_2 的**交集**, 用 $A_1 \cup A_2$ 记 A_1 与 A_2 的**并集**. "a 是 A 的元"简记为 $a \in A$.

现在设 G 与 G' 是两个群, 而 f 是从 G 到 G' 的映射. 如果对于所有的 σ, $\tau \in G$, 总有 $f(\sigma\tau) = f(\sigma)f(\tau)$, 这样的 f 称为从 G 到 G' 的**同态映射**. 容易看出 $f(1) = 1$ 与 $f(\sigma^{-1}) = (f(\sigma))^{-1}$.

如果 N' 是 G' 的子群, 那么原象 $N = f^{-1}(N')$ 是 G 的子群. 其实, σ, $\tau \in N$ 的意义就是 $f(\sigma)$, $f(\tau) \in N'$. 但是又有 $f(\sigma\tau) = f(\sigma)f(\tau) \in N'$, 所以 $\sigma\tau \in N$. 同理 $\sigma^{-1} \in N$. 如果 N' 是 G' 的正规子群, 那么 N 也是 G 的正规子群, 因为由 $\sigma \in G$, $\tau \in N$ 得到

$$f(\sigma\tau\sigma^{-1}) = f(\sigma)f(\tau)(f(\sigma))^{-1} \in f(\sigma)N'(f(\sigma))^{-1} = N',$$

所以$\sigma\tau\sigma^{-1}\in N$.

仿此可证G的子群N的象N'是G'的子群．如果N是G的正规子群，而映射f又是映成G'的，那么由$\sigma'\in G'$，$\tau'\in N'$，就能求得元$\sigma\in G$，$\tau\in N$，使得$f(\sigma)=\sigma'$，$f(\tau)=\tau'$．因为f应用于$\sigma\tau\sigma^{-1}$，就得到$\sigma'\tau'\sigma'^{-1}\in N'$．所以$N'$是$G'$的正规子群.

因为G'的单位元是G'的正规子群，所以它的原象K是G的正规子群．K称为同态f的核．它是由适合$f(k)=1$的G中那种元k组成的．现在来决定G中哪些元经f作用有相同的象．方程$f(\sigma)=f(\tau)$等价于$f(\sigma\tau^{-1})=1$，即$\sigma\tau^{-1}\in K$，或$\sigma\in K\tau=\tau K$．因此，正好是模K的一个旁系中所有元有相同的象．现在把每个旁系σK与元$f(\sigma)\in f(G)$对应，$f(\sigma)$是σK中所有元共同的象．这样就存在映商群G/K成G的象$f(G)$的一个可逆单值映射．容易看出这映射也是同态．因为它是可逆单值的，所以它就是G/K与$f(G)$之间的同构.

最后指出，G的每个正规子群N可以作为一个同态的核．把G映成商群G/N，这时$f(\sigma)=\sigma N$．直接看出f是同态，它把每个元映成此元所属的那个旁系．G/N的单位元是N，所以其原象就是N这集．因此N是这映射f的核，这种映射称为映G成G/N的**典范同态**

命题 35　设f为映G成G'的同态，N为G的正规子群，并且$N'=f(N)$．那么以典范方式由f导出映G/N成G'/N'的同态g．如果还有$N=f^{-1}(N')$，那么这同态是同构.

证　把旁系σN在g作用下的象定义为$f(\sigma N)=f(\sigma)N'$．直接看到g是同态．由于f是映成的映射，得到G/N是映成G'/N'的．如果来决定此同态的核：当$f(x)N'=N'$，因此

$f(x)\in N'$，即 x 属于 $f^{-1}(N')$ 时，那么 xN 属于核．因此，如果 $f^{-1}(N')=N$，那么就必定是 $x\in N$，并且就有 $xN=N$．这时同态的核就是 G/N 的单位元．所以同态就是同构．

命题 36 设 H 为 G 的子群，并且 N 是 G 的正规子群．那么 $H\cap N$ 是 H 的正规子群，并且商群 $H/H\cap N$ 与(G/N 的子群)HN/N 同构．

证 设 f 为映 G 成 G/N 的典范同态．把映射 f 限制在子群 H 上，得到映 H 到 G/N 的同态 g．象集 $g(H)$ 由 $\sigma\in H$ 的旁系 σN 组成，并且容易看出它就是商群 HN/N．g 的核是 $H\cap N$．因此 $H\cap N$ 是 H 的正规子群，并且商群 $H/H\cap N$ 同构于同态 g 作用于 H 的象．

系 G, H 与 N 如上命题所设，如果 G/N 是 Abel 群，那么 $H/H\cap N$ 也是 Abel 群．

定义 如果群 G 具有递降的子群链

$$G=G_0\supset G_1\supset G_2\supset\cdots\supset G_s=1,$$

对于 $i=1, 2, \cdots, s$, G_i 是 G_{i-1} 的正规子群，并且商群 G_{i-1}/G_i 都是 Abel 群，群 G 就称为**可解的**．

命题 37 可解群的子群都是可解的．

证 设 G 是可解的，G_i 是属于它的正规子群链．设 H 是 G 的子群，并且 $H_i=H\cap G_i$．于是也有

$$H_{i-1}\cap G_i=H\cap G_{i-1}\cap G_i=H\cap G_i.$$

G_i 是 G_{i-1} 的正规子群，并且 H_{i-1} 是 G_{i-1} 的子群．因为 G_{i-1}/G_i 是 Abel 群，由命题 36 的系，所以 $H_{i-1}/H_{i-1}\cap G_i$ 也是 Abel 群．但此群就是 H_{i-1}/H_i．

命题 38 可解群的同态象是可解的．

证 设 G 是可解的，G_i 是属于它的正规子群链．设 f 为同态，$G'=f(G)$．来证明 $G'_i=f(G_i)$ 就是属于 G' 的正规子群

链. 限制 f 在 G_{i-1} 上得到映 G_{i-1} 成 G'_{i-1} 的同态. G_i 是 G_{i-1} 的正规子群, G'_i 是 G_i 的象. 根据命题 35, 由此又导出映 G_{i-1}/G_i 成 G'_{i-1}/G'_i 的同态映射. 而今 G_{i-1}/G_i 是 Abel 群, 而 Abel 群的同态象显为 Abel 群.

现在要证阶为素数幂的群是可解的. 对于它的证明还需要几个群论概念.

设 G 为群. 其两元 a 与 b 称为**共轭的**, 是指, 有 $x\in G$, 使得 $b=xax^{-1}$. 容易看出, 每个元与自身共轭; 如果 a 与 b 共轭, 那么 b 与 a 也共轭; 如果 a 与 b 共轭并且 b 与 c 共轭, 那么 a 与 c 也共轭. 这说明共轭是个等价关系. 于是, 群 G 就可以由一些互不相交的类所盖满, 每个类中的元互为共轭, 但绝不与另一类的元共轭, 一个类可以正好只由一个元组成. 如果对于所有的 $x\in G$, 都有 $xax^{-1}=a$, 就正是这种情况. 也就是 $xa=ax$, 因此元 a 与每个元 $x\in G$ 都是可交换的. 容易看到, 这些元 a 的集 Z 构成 G 的一个 Abel 子群, 称为 G 的**中心**. Z 当然与 G 的任何元都是可以交换的, 所以 Z 是 G 的正规子群.

设 $a\in G$. 为了得到与 a 共轭的元, 就需要把所有的 xax^{-1} 都算进去, 其中 x 遍历群 G. 不同的 x 可以正好生成相等的共轭元. 方程 $xax^{-1}=yay^{-1}$ 与 $(y^{-1}x)a=a(y^{-1}x)$ 等价, 因此等价于元 a 与 $y^{-1}x$ 的可交换性. 现在设 N_a 是由所有与 a 可交换的元 z 组成的集, 因此上述方程就可以写成 $y^{-1}x\in N_a$, 或 $x\in yN_a$. 容易证实 N_a 是个群. 因此就证明了: 旁系 yN_a 中的元 x 正好就是那些把 a 变换成同一共轭元的元. a 的不相同的共轭元的个数, 换句话说, 含有 a 的那类中元的个数就等于 N_a 的旁系的个数. 现在设 G 是个阶为 n 的有限群. 那么每一类中元的个数就是 n 的因子. 这些类盖满了群 G, 因

此这些类中元的个数的和就是 n. 只含一个元的类有 z 个, z 就是中心的阶. 于是得到形如

$$n=z+d_1+d_2+\cdots$$

的公式, 其中 d_i 是 n 的异于1的因子. 如果现在设 $n=p^r$, $r\geqslant 1$, 并且 p 为素数, 那么 n 与所有的 d_i 都被 p 整除, 所以 z 也被 p 整除. 但是这就指明此群 G 具有非平凡中心 Z. 而今容易按 r 用归纳法来证明这种群 G 的可解性. 阶为 p 的群总是 Abel 的,所以可解. 商群 G/Z 有小于 n 的素数幂阶, 因此可以假设它的可解性已得证. 设 G_i/Z 是 G/Z 的正规子群链来示明其可解性. 设 f 为映 G_{i-1} 成 G_{i-1}/Z 的典范同态. G_{i-1} 中 Z 所有旁系的原象就是这些旁系的并集. $G_i/Z=N'$ 是 G_{i-1}/Z 的正规子群,其商群是 Abel 的,并且 N' 的原象就是 G_i. 于是 G_i 是 G_{i-1} 的正规子群, 并且它的 f 象还是 N'. 根据命题 35, 商群 G_{i-1}/G_i 与 G_{i-1}/Z 中 G_i/Z 的商群同构, 所以是 Abel 的. 这些 G_i 现在就作出一个递降的正规子群链, 其末项为 Z 本身. 再加一个群 1, 因为 Z 是 Abel 群, 所以 G 具有正规子群链,这就证明了 G 的可解性.

因此证明了

命题 39 素数幂阶的群是可解的.

与此相反,要指明某些群的不可解性.

设 M 为有限集, φ 是把 M 映成自身的一个一一映射. 这样的映射称为 M 的一个**置换**. 如果 φ 与 ψ 是 M 的置换, 那么 $\varphi\psi$(先 ψ 后 φ)与 φ^{-1} 也是置换. 由于映射的相继施行显然有结合律, 于是 M 的置换就作成一个群. 如果 n 是 M 中元的个数, 这个群就称为 n 元的**对称群**并记作 S_n. 它的阶是 $n!$. S_n 的子群称为**置换群**. 如果 a, b, c 是 M 中的三个不同的元, 那么就用记法(a, b, c)表示 M 的一个这样的置

换：把 a 映成 b，b 映成 c 与 c 映成 a，而 M 中其它所有元都不动. (a, b, c) 称为一个**三项循环**. $(a, b, c)^{-1}=(c, b, a)$. 现在来证明下列的

引理 设 G 为至少 5 元的置换群，它包含每个三项循环，并且 N 是 G 的带 Abel 商群的正规子群. 那么 N 也一定包含每个三项循环.

证 设 f 为映 G 成 G/N 的典范同态，(a, b, c) 是任一三项循环. 在 M 中再取两个元 d 与 e. 令 $x=(d, b, a)$，$y=(a, e, c)$. $x^{-1}y^{-1}xy$ 的 f 象是 $x'^{-1}y'^{-1}x'y'$，其中 x' 与 y' 分别是 x 与 y 的象. 因为假设象群是 Abel 的，所以这个象就是 1. 于是 $x^{-1}y^{-1}xy$ 属于 f 的核. 而今

$$x^{-1}y^{-1}xy=(a, b, d)(c, e, a)(d, b, a)(a, e, c)$$
$$=(a, b, c).$$

命题 40 $n\geqslant 5$ 的对称群 S_n 是不可解的.

证 设有一个从 S_n 开始的带有 Abel 商群的正规子群链存在. 因为 S_n 包含所有的三项循环，由引理得知，这链中的每个群必定包含所有的三项循环. 因此，这样的一个链就不可能用 1 这群来结束.

B. 方程用根式的可解性

为了避免由特征造成困难，下列命题只限于特征为 0 的体.

设 K 为体，K_i 是由扩体组成的、以 F 为末项的递升序列：

$$K=K_0\subset K_1\subset K_2\subset\cdots\subset K_s=F.$$

如果对于 $i=1, 2, \cdots, s$，$K_i=K_{i-1}(\alpha_i)$，其中 α_i 是 K_{i-1} 中多项式 $x^{n_i}-a_i$ 的一个根，那么 K 的扩张 F 称为**根式扩张**.

如果 K_i 是具有 Abel 自同构群的、K_{i-1} 上的正规扩张，扩张 F 称为半 **Abel 的**.

引理 1 K 的根式扩张 F 可以嵌入一个半 Abel 扩张之中.

证 设 F 是 K 的根式扩张，K_i 是相应的体序列. 又设 m 是所有 n_i 的最小公倍. 把 m 次原根 ε 添加于 F. 考虑体链:

$$K_0 = K \subset K_0(\varepsilon) \subset K_1(\varepsilon) \subset \cdots \subset K_s(\varepsilon) = F(\varepsilon).$$

紧接在命题 27 之前已证明 K 上的 $K(\varepsilon)$ 的自同构群是 Abel 的. 体 $K_i(\varepsilon)$ 是由 α_i 添加于 $K_{i-1}(\varepsilon)$ 得到的. 因为 $K_{i-1}(\varepsilon)$ 含有 n_i 次原根，由命题 32, $K_{i-1}(\varepsilon)$ 上的 $K_i(\varepsilon)$ 的自同构群还是循环的. 因此 $F(\varepsilon)$ 就是 K 的半 Abel 扩张，它包含 F.

引理 2 设 F_1 与 F_2 都是 K 的半 Abel 扩张，并且都包含在 K 的一个扩张之中. 那么由 F_1 与 F_2 合成的体 F_1F_2 也是 K 的半 Abel 扩张.

证 设

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = F_1,$$

$$K = K'_0 \subset K'_1 \subset \cdots \subset K'_t = F_2$$

是相应的体链. 作新链

$$K = K_0 \subset K_1 \subset \cdots \subset K_s$$

$$= F_1K'_0 \subset F_1K'_1 \subset \cdots \subset F_1K'_t = F_1F_2.$$

由假设，K_{i-1} 上的 K_i 的自同构群是 Abel 的. 只要证明 $F_1K'_{i-1}$ 上的 $F_1K'_i$ 的自同构群是 Abel 的. 由假设，K'_{i-1} 上的 K'_i 的自同构群是 Abel 的. $F_1K'_{i-1}$ 是 K'_{i-1} 的扩张，它与 K'_i 的合成是体 $F_1K'_i$. 由命题 34, $F_1K'_i$ 就是 $F_1K'_{i-1}$ 的正规扩张，其自同构群与 K'_{i-1} 上的 K'_i 的自同构群的一个子群同构. 所以这个群也是 Abel 的，于是 F_1F_2 是 K 的半 Abel 扩张.

引理 3 设 F 是 K 的半 Abel 扩张. F 就可以嵌入 K 的一个正规的、半 Abel 扩张之中.

证 体 F 是可分的. 于是 F 可以嵌入一个正规扩张 Ω 之中. 设 $F_1, F_2, \cdots, F_s$ 是 K 上在 Ω 的所有自同构下 F 的象, 并且 $\Omega_0=F_1F_2\cdots F_s$ 是由这些象合成的体. 作为 F 的每个同构象 F_i 是半 Abel 的, 由引理 2 指出 Ω_0 也是 K 的半 Abel 扩张, 它当然包含 F. 因此还只要证明 Ω_0 是 K 的正规扩张. 现在每个映 Ω_0 到 Ω 的同构是由 K 上的 Ω 的自同构 σ 生成的. σ 不过置换这些体 F_i, 因此把 Ω_0 变换成本身. 于是每个映 Ω_0 到 Ω 的同构就是 Ω_0 的自同构. 所以 Ω_0 是 K 的正规扩张.

定义 设 $f(x)$ 是 K 中的不可约多项式. 如果有 K 的一个根式扩张存在, 其中含有 $f(x)$ 之一根, 那么 $f(x)$ 称为**用根式可解**.

命题 41 设 $f(x)$ 是 K 中的不可约多项式, E 是 $f(x)$ 的分裂体, 具有自同构群 G. 那么, $f(x)$ 用根式可解, 当且仅当群 G 是可解的, 并且还存在 K 的一个根式扩张, $f(x)$ 在其中分解成线性因子.

证 1. 如果 $f(x)$ 用根式可解, 那么存在 K 的根式扩张, 其中含 $f(x)$ 之一根 α. 根据引理 1 与 3, 就存在 K 的正规的、半 Abel 扩张 Ω_0, 其中有 $f(x)$ 的根 α. 由命题 15 的系, $f(x)$ 在 Ω_0 中可以分解成线性因子. 所以 Ω_0 包含 $f(x)$ 的分裂体 E'. K 上的 Ω_0 的自同构群是可解的, 并以 K 上的 E' 的自同构群作为其商群, 即作为其同态象. 根据命题 38, 所以这个在 K 上的 E' 的自同构群是可解的. 如果 E 是原来给定的那个对于 $f(x)$ 的分裂体, 那么 E 与 E' 同构, 因此也有同构的自同构群.

2. 设$f(x)$的分裂体E的自同构群G是可解的；n是G的阶. ε为n次原根并且$K'=K(\varepsilon)$. 显然K'是K的根式扩张. 体$E'=EK'$是K'上$f(x)$的分裂体，由命题34，K'上的E'的自同构群G'与G的子群同构，因此，由命题37，G'也是可解的. 设

$$G'=G_0\supset G_1\supset G_2\supset\cdots\supset G_s=1$$

是带Abel商群的正规子群链. 相应于E'的不动点体作成体的递升序列：

$$K'=K'_0\subset K'_1\subset K'_2\subset\cdots\subset K'_s=E'.$$

于是E'是K'_{i-1}的正规扩张，其自同构群是G_{i-1}. 因为G_i是G_{i-1}的正规子群，K'_i就是K'_{i-1}的正规扩张，其自同构群G_{i-1}/G_i是Abel的. 因为K'_{i-1}含n次原根，K'_i是K'_{i-1}上的Kummer体，所以是通过根式的添加得到的. 立即看出K'_i是K'_{i-1}的根式扩张. 总起来E'就是K的根式扩张，并且$f(x)$在E'中分解成线性因子.

C. 方程的Galois群

本节考虑的体特征仍可以是任意的.

设K为体，$f(x)$是K中的没有重根的多项式，E是$f(x)$的分裂体，并且$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$是$f(x)$在$E$中的分解. $\alpha_1, \alpha_2, \cdots, \alpha_n$是$E$的生成元. 已经注明过，$K$上的$E$的自同构群$G$中每个元$\sigma$可以$\sigma$作用于全部$\alpha_i$的效果唯一地描写出来. σ置换这些元α_i，因此，可以把G看成n个元的集的置换群. 为了简明起见，只需把G当作α_i的指标i的置换群，使得G是置换这些数码1, 2, $\cdots$, n的，如此了解，通常把G记为方程$f(x)=0$的**Galois 群**. $f(x)$这多项式并不需要在K中不可约. 设$p(x)$为$f(x)$在K中的不可约因

子. G 中元 σ 只能把 $p(x)$ 之一根换成 $p(x)$ 的另一根. 另一方面, 如果 α_i 与 α_j 是 $p(x)$ 的两个根, 那么两个体 $K(\alpha_i)$ 与 $K(\alpha_j)$ 同构, 并且此同构可以通过 G 之一元来实现. 经过根的重行编码还可以假设 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 $p(x)$ 所有的根. 于是 G 的元一方面把数字 $1, 2, \cdots, r$ 只置换为本身; 另一方面, G 的适当元把这前 r 个数字的任一个换成这前 r 个数字中任何另一个. 数字 $1, 2, \cdots, n$ 的具有这种性质的子集称为 G 的**可迁区**. 显然这些数字 $1, 2, \cdots, n$ 划分为互不相交的可迁区, 它们对于 $f(x)$ 的那些不可约因子有个一一对应的关系. 因此, 如果知道置换群 G, 那么由此可以得到 $f(x)$ 在 K 中分解的不可约因子. $f(x)$ 是不可约的, 当且仅当数字 $1, 2, \cdots, n$ 作成一个单独的可迁区. 于是群 G 称为可迁的. 如果 U 为 G 的子群并且 B 是所属的不动点体, 那么把 $f(x)$ 当作 B 中的多项式, U 是 $f(x)$ 的 Galois 群. U 的那些可迁区就与 $f(x)$ 在 B 中分解的不可约因子对应.

设 $f(x)$ 在 K 中不可约, 群 G 是可迁的. 设 U 为 G 的正规子群, B 就是 K 的**正规扩张**. 在 B 中选取 $f(x)$ 的某个不可约因子 $p(x)$. 如果 σ 是 G 的元, σ 就实现为 B 的自同构. 因此, 象 $\sigma(p(x))$ 还是 B 中的不可约因子. 现在 G 是可迁的. 于是有 $\sigma\in G$, 它把 $p(x)$ 之一根变换成 $f(x)$ 的另一根. 因此在 B 中的 $f(x)$ 每个不可约多项式就形如 $\sigma(p(x))$. 由此得知, U 的可迁区都有相等的长度. 如果 n 为素数, 那么或者 U 本身是可迁区, 要不其所有可迁区的长度都是 1, 即 U 只由恒同元组成. 因为这个结果以后有用, 把它系统地阐述作为

命题 42 如果 G 是数字 $1, 2, \cdots, q$ 的可迁置换群, 其中 q 是素数, 那么 G 的每个异于 1 的正规子群就还是可迁的.

定义 设 k 为体，$u_1, u_2, \cdots, u_n$ 是无关的变量，并且 $K=k(u_1, u_2, \cdots, u_n)$ 是以 k 中元为系数的 $u_1, u_2, \cdots, u_n$ 所有有理函数构成的体. 属于 K 的多项式

$$f(x)=x^n+u_1x^{n-1}+\cdots+u_n$$

称为 k 上的 n 次**一般方程**.

现在来决定 n 次一般方程的 Galois 群. 决定 $f(x)$ 的分裂体 E'，并且在 E' 中假设

$$f(x)=(x-\xi_1)(x-\xi_2)\cdots(x-\xi_n).$$

u_i 是 ξ_j 的多项式，u_i 就是用 $(-1)^i$ 乘每取 i 个不同的根 ξ_j 的所有积之和. 另一方面，在第 II 部分 G 段中已经考虑过下列的例：取 n 个独立变量 $x_1, x_2, \cdots, x_n$，并且来看体 $E=k(x_1, x_2, \cdots, x_n)$ 与多项式

$$g(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$$
$$=x^n+a_1x^{n-1}+\cdots+a_n.$$

在 E 中考虑过 x_i 的 $n!$ 个置换并且证明了它们的不动点体就是 $k(a_1, a_2, \cdots, a_n)$. a_i 表成 x_j 的方式与 u_i 表成 ξ_j 是同样的.（这里并不需要对称函数的那个更精确的多项式性质.）

设 $\varphi(u_1, u_2, \cdots, u_n)$ 是以 k 中元为系数的 u_i 的多项式，它具有这种性质：对于 $u_i=a_i$，其值为 0，即 $\varphi(a_1, a_2, \cdots, a_n)=0$. 把 a_i 的 x_j 表式代入，就得出 x_i 的一个表式，其中所有项都抵消了. 把其中的每个 x_i 代以 ξ_i，那么也得到一个表式，其中所有项消失，因此就是零多项式. 但是这种代入单纯用 u_i 代 a_i 就完成了，所以原来的多项式 $\varphi(u_1, u_2, \cdots, u_n)$ 就必定已经是零多项式.

于是证明了，不同的多项式 $\varphi(u_1, u_2, \cdots, u_n)$ 有不同的值 $\varphi(a_1, a_2, \cdots, a_n)$. 把每个多项式 $\varphi(u_1, u_2, \cdots, u_n)$ 对应于其值 $\varphi(a_1, a_2, \cdots, a_n)$ 就给出映 u_i 的多项式成 a_i 的多项式

的一个一一映射. K 由 u_i 的多项式的商组成, 体 $k(a_1, a_2, \cdots, a_n)$ 由 a_i 的多项式的商组成. 读者容易证实, 经过考虑得到映 K 成 $k(a_1, a_2, \cdots, a_n)$ 的同构, 使得 k 中元不动而把每个 u_i 映成 a_i. 而且多项式 $f(x)$ 的象是 $g(x)$ 这个多项式. 根据命题 10, 这同构可以开拓成 E 与 E' 间的同构, 它把 $f(x)$ 的这些根 ξ_i 映成 $g(x)$ 那些根 x_i 可以取得的编码.

现在 $k(a_1, a_2, \cdots, a_n)$ 是对称群 S_n 的不动点体. 由已证得的同构得出著名的 **Abel** 命题:

命题 43 k 上的 n 次一般方程的 Galois 群就是对称群 S_n. 如果 k 的特征是 0 而且 $n \geqslant 5$, 那么 n 次一般方程不是由根式可解的.

本命题的后一部分由命题 40 与 41 得到.

可以提出这样的问题: 先给定任一置换群, 是否可以把它作为某个适当的方程的 Galois 群. 其实, 由适当地选择基体是可能的. 设 G 是给定的 n 个数字的一个置换群, $f(x)$ 是 k 上的 n 次一般方程, 并且照前面来定义两个体 K 与 E'. G 是 S_n 的子群, 从而得到 G 是 $f(x)$ 的 Galois 群, 如果把 $f(x)$ 看成是 G 的不动点体 B 中的多项式. 因为每个有限抽象群可以表示成置换群, 因此还得出适当基体的正规扩张, 其自同构群是同构于给定的抽象群的. 与此对立的是一个还未解决的问题: 是否在有理数体上有这样的正规扩张存在.

设 K 是任一体, $f(x)$ 是 K 中的素数 q 次的不可约多项式, 它的 Galois 群设为可解的. 将要证明如此情况下 G 的结构特别简单. 首先, 因此存在正规子群链

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = 1,$$

其中相继的商群都是 Abel 的. 尤其 G_{s-1} 本身就是个 Abel 群. 因为 G_{s-1} 的每个子群是 G_{s-1} 的正规子群, 当然包含异

于1的循环子群，因此可以假定$G_{s-1}\neq 1$并且是循环的，因为必要时还可以在链中加进一个群．设G_{s-1}是由σ生成的循环群．因为群G是可迁的，由命题42知道，每个群G_i，尤其是G_{s-1}都是可迁的．σ的幂次构成G_{s-1}，由可迁性，它们把数字1换成所有其它的数字．如果$\sigma^i(1)=\sigma^j(1)$，那么$\sigma^{i-j}(1)=1$．如果d是适合$\sigma^d(1)=1$的最小正数，那么这些数字1，$\sigma(1)$，$\sigma^2(1)$，…，$\sigma^{d-1}(1)$就是所有不同的数字，并且是由σ的幂可能换成的全部数字．于是，由可迁性得到必定$d=q$．适当的编码可得到数字1，2，…，q按次序正好就是这些数字1，$\sigma(1)$，$\sigma^2(1)$，…，$\sigma^{q-1}(1)$．对于$i\leqslant q-1$，就有$\sigma(i)=i+1$．由$\sigma^q(1)=1$得到$\sigma(q)=1$．显然用剩余类体Q_q的元来代替这些数字更为适用，因为这时对每个数字就有公式$\sigma(x)=x+1$．当然有$\sigma^i(x)=x+i$．如果a，b是Q_q的元，$a\neq 0$，那么函数$\Phi(x)=ax+b$就是把Q_q映成本身的一一映射，因此是个置换．

定义 设Q_q的一个置换群中每个置换具有形式

$$\tau(x)=ax+b,\quad a,\ b\in Q_q,\ a\neq 0,$$

并且这群中还含有特殊的置换$\sigma(x)=x+1$，这种群就称为**线性的**．

设$a\neq 0$，1并且$\tau(x)=ax+b$．于是有

$$\tau^2(x)=a^2x+ab+b.$$

由归纳法得出

$$\tau^i(x)=a^ix+(a^{i-1}+a^{i-2}+\cdots+1)b.$$

因为$a\neq 1$，这个式子也可写成形式$\tau^i(x)=a^ix+\dfrac{a^i-1}{a-1}b$．因为$a\neq 0$，在$Q_q$中$a^{q-1}=1$成立，从而得$\tau^{q-1}(x)=x$．于是$\tau$的阶是$q-1$的因子，正好看出它就是使得$a^i=1$的最小的$i$．

对于 $a=1$ 并且 $b\neq 0$, 就成为 $\tau(x)=x+b$, $\tau^i(x)=x+ib$, 因此 τ 具有阶 q.

因此线性群中只有那些异于 1 的 σ 的幂才具有阶 q, 其中 σ 如前所述, $\sigma(x)=x+1$.

引理 设 H 是 q 个数字的置换群, q 为素数, N 是 H 的正规子群而且 N 是线性群. 那么 H 就是线性群.

证 N 含有置换 σ. 设 τ 是 H 的某一置换. 那么 $\tau\sigma\tau^{-1}$ 是 N 的元, 它具有阶 q. 因此它是异于 1 的 σ 的幂, 设 $\tau\sigma\tau^{-1}=\sigma^a$, a 不能被 q 整除. 因此 $\tau\sigma=\sigma^a\tau$, 从而 $\tau\sigma(y)=\sigma^a\tau(y)$. 由此得 $\tau(y+1)=\tau(y)+a$. 又得到 $\tau(y+2)=\tau(y)+2a$, 一般有 $\tau(y+x)=\tau(y)+ax$. 取 $y=0$ 并且 $b=\tau(0)$, 故得 $\tau(x)=ax+b$. 所以 H 是线性的.

命题 44 如果一个素数次的不可约方程的 Galois 群 G 是可解的, 那么 G 就是线性的.

证 群 G_{s-1} 由 σ 的幂组成, 因此就是线性的. 把上述引理重复应用到正规子群链, G 就是线性的.

设 G 为线性群, $\tau\in G$, $\tau(x)=ax+b$. 因此 $\tau'=\sigma^{b'-b}\tau$ 也在 G 中, 而且形如 $\tau'(x)=ax+b'$. 于是, 如果由 G 中的一个 τ 给定了 a, 那么带有所有可能的 $b\in Q_q$ 的置换就都在 G 中. 尤其是 $\tau_a(x)=ax$. 显然 $\tau_{a_1}\cdot\tau_{a_2}=\tau_{a_1a_2}$, 这就指出, 所出现的 a 作成乘法群. 这个乘法群是 Q_q 中异于 0 的那些元组成的乘法群的子群, 它是循环的而且其阶 d 是 $q-1$ 的因子. 给定了 d, 与它联系着的 a 不过就是 Q_q 中所有的 d 次单位根. G 的阶就是 dq, G 的结构因 dq 的给定而唯一决定. 尽可能大的阶是 $(q-1)q$.

命题 45 每个线性群是可解的.

证 设 G 是线性的, N 是由 σ 生成的循环子群. 对所有

的 $\tau \in G$ 有 $\tau\sigma\tau^{-1}=\sigma^a \in N$，所以 N 是 G 的正规子群. G 的可解性在于证明 G/N 是 Abel 的. 如果 τ_a 是置换 $\tau_a(x)=ax$，那么旁系 $N\tau_a$ 是由固定 a 的那些置换 $\tau(x)=ax+b$ 组成的. 因此这些旁系就是不同的 $N\tau_a$. 现在有 $N\tau_{a_1}\cdot N\tau_{a_2}=N\tau_{a_1}\tau_{a_2}=N\tau_{a_1a_2}=N\tau_{a_2}\cdot N\tau_{a_1}$，因此已得证明.

设 $\tau(x)=ax+b$. 找出 τ 的不动点，就是求方程 $ax+b=x$ 的解. 对于 $a\neq 1$，解就是 $\dfrac{-b}{a-1}$；对于 $a=1$ 并且 $b\neq 0$，就没有不动点；$a=1$，$b=0$ 就是恒同映射. 因此，G 中异于恒同映射的置换不能有两个不动点.

现在设 α_i 与 α_j 是 $f(x)$ 两个不同的根. 考察中间体 $K(\alpha_i, \alpha_j)$. 所属子群的元 τ 应当使 α_i 与 α_j 都不动，因此有两个不动点. 根据上述，$\tau=1$. 这说明体 $K(\alpha_i, \alpha_j)$ 是 $f(x)$ 的分裂体 E. 由此已证明

命题 46 如果素数次不可约方程的群 G 是可解的，那么分裂体通过两个根的添加就已经生成了.

由此命题来作点应用. 设 K 是实数体的子体(因此 K 尤其具有特征 0)，$f(x)$ 是 K 中的奇素数次不可约方程，设它是用根式可解的. 再设这多项式有两个实根. 把它们添加于 K 得到一个实数体，由命题 46，它就是 $f(x)$ 的分裂体. 因此 $f(x)$ 只有实根. 在一般情况，一个这样的方程只有实根或只有一个实根. 于是得到

系 一个实数体中的奇素数次不可约方程如果是用根式可解的，那么它或者恰有一个实根，要不就全是实根.

读者不难找到有理系数的 5 次方程，它在 Q 中不可约而且恰有三个实根. 一个这样的方程就不是用根式可解的. 多项式 $x^5-10x-2$ 是这种类型的一个例子.

D. 规 尺 作 图

作图题就是要从一个给定的几何对象导出另一个几何对象. 这时, 几何对象应受条件限制, 使其性质可由有限个点和线段画出来(例如: 三角形的三个顶点; 圆的中心及其半径).

如果作图可以分成有限步, 每步都在一个固定的平面上, 并且每步画出下列可能性之一, 就说这种作图可以用圆规与直尺来实现:

1. 由前些步在这平面上所决定的区域中任取一点.

2. 过两个已作出的点或两个选择的点作相连直线.

3. 以先作出的点为中心过先作出的点作圆.

4. 决定先作出的两直线的交点, 或者已经作出的直线与已经作出的圆的交点, 或者两个这样的圆的交点.

条件 1 显然必要, 因为必须在空平面上开始选择一点. 这时, 设想在这平面上给定了这样的一些线段, 它们描绘了原有几何对象的性质, 并且通过作图应当得到描绘要作的几何对象的线段. 下文简述如何把几何问题换成代数问题.

设想在平面上引入一个直角坐标系, 从原点在正 x 轴上画出给定的线段. 其终点可在 x 轴上的值为 $a_1, a_2, \cdots, a_r$. 这就可以作图. 一定数目的 i 个步骤以后, 就可以画出一定的点集. 所有作出的点的坐标集合记为 $b_1, b_2, \cdots, b_s$; a_ν 组成其子集. 把 $b_1, b_2, \cdots, b_s$ 添加于有理数体 Q 就得到一个实数的体 K_i. 至此为止作出的直线与圆已经化为方程, 其系数是 K_i 中元. 论到第 $i+1$ 步, 只有它是(前所述的四种可能性中)第 1 类型或第 4 类型才可能有新点出现. 如果它是第 1 类, 把那点取成有理数坐标是可以作到的, 此时便有 $K_{i+1}=K_i$. 如果有第 4 类的点, 那么通过交点的计算, 最可能出

现的不过是 K_i 中元的平方根，因此，或者是 $K_{i+1}=K_i$，要么就是 $(K_{i+1}/K_i)=2$. 如果描绘要作的几何对象的线段已从原点画到正 x 轴上，作图就算完成了. 设这些线段终点的坐标为 $\xi_1, \xi_2, \cdots, \xi_t$. 如果 n 是作图(步骤)的全长，那么 K_n 就是含有 $\xi_1, \xi_2, \cdots, \xi_t$ 的体. 如果把 $K=Q(a_1, a_2, \cdots, a_r)$ 看成基体，那么 K_n 这个体就是 K 的半 Abel 扩张，其中的每个部分扩张都是二次的. 这时，读者回到第 III 部分 B 段中那些引理的证明. 如果在引理 2 中还假设那两个扩张 F_1 与 F_2 的每个部分扩张都是二次的，那么扩张 F_1F_2 就有同样的性质，正是因为 $F_1K'_{i-1}$ 上的 $F_1K'_i$ 的群同构于 K'_{i-1} 上的 K'_i 的群的子群. 于是，引理 3 的证明指出 K_n 可以嵌入 K 的一个正规扩张 Ω 之中，这个 Ω 可以从 K 经过逐次的二次扩张得到. Ω 这个体显然包含 $F=K(\xi_1, \xi_2, \cdots, \xi_t)$，因此也包含那个含有体 F 的、K 的最小正规扩张 E. 作为 Ω 的次数是 2 的幂，从而 F 与 E 这两个体也是如此.

其论点如下：不依靠几何的作图可以从几何问题本身读出要作的量 $\xi_1, \xi_2, \cdots, \xi_t$ 的性质. 因此，这两个体 E 与 F 的代数性质必须由几何问题来决定. 如果这时 (F/K) 或 (E/K) 不是 2 的幂，那么根据上段所论，规尺作图就不可能.

现需证明

命题 47 设 $a_1, a_2, \cdots, a_r$ 是一个几何问题的数据，$\xi_1, \xi_2, \cdots, \xi_t$ 是要作出的量，并设 $K=Q(a_1, a_2, \cdots, a_r)$. 如果所有的 ξ_i 都是 K 上的代数元，并且含有这些 $\xi_1, \xi_2, \cdots, \xi_t$ 的、K 的最小正规扩张的次数是 2 的幂. 那么这个几何问题正好就是可以用规尺来解决的.

证 条件的必要性已经证明了. 因此，假设 (E/K) 是 2 的幂，要证 E 的每个元都是"可作的". K 上的 E 的自同构

群 G 根据命题 39 是可解的．于是有正规子群链

$$G=G_0\supset G_1\supset\cdots\supset G_s=1,$$

使得每个商群 G_{i-1}/G_i 都是 Abel 的．每个都有 2 的幂作为其阶．如果阶大于 2，就有 2 阶的子群 H/G_i．因此可把 H 这个新的群插入 G_{i-1} 与 G_i 之间．这就可以假定所有的商群的阶都是 2．属于这个递降群链的是递升体链

$$K=K_0\subset K_1\subset\cdots\subset K_s=E.$$

这时的困难在于这些体不一定是实数的．如果一个复数的实部与虚部都是可作的，即称之为可作的复数．读者在中学时当然学过，怎样从长为 a 与 b 的线段来作出长为 $a\pm b$, ab, $\frac{a}{b}$ 的线段(用相似三角形法)．也能作出长为$\sqrt{a}$ 的线段(用比例中项法)．因此，由这些给定的数据就可以把 K 的每个元作出来．设 K_{i-1} 中所有元的可作性已经证明了．因为 $(K_i/K_{i-1})=2$，可由$\sqrt{\alpha}$ 的添加得到 K_i，其中 α 是一个已经作出了的复数．在 Gauss 数平面上这是平分一角与画出一个正的可作数的平方根来实现的．于是 K_i 也是可作的，按 i 作归纳法就证明了本命题．

例 1．内接于半径为 1 的圆的正 n 边形的作图． 这里 $K=Q$, $\xi_1=\cos\frac{2\pi}{n}$, $\xi_2=\sin\frac{2\pi}{n}$．与它等价的就是

$$\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n},$$

即 n 次原根的作图．$E=Q(\varepsilon)$ 已经是 Q 的正规扩张，因此只须找出这个扩张的次数．根据命题 27，这个次数是 $\varphi(n)$．设 $n=p_1^{\nu_1}p_2^{\nu_2}\cdots p_r^{\nu_r}$ 是 n 分解成不同素数幂．那么就有

$$\varphi(n)=p_1^{\nu_1-1}(p_1-1)p_2^{\nu_2-1}(p_2-1)\cdots p_r^{\nu_r-1}(p_r-1).$$

如果 $p_1=2$，指数 ν_1 就是任意的．但是如果 p_i 是奇数，那就

必须$\nu_i=1$，而且还必须p_i-1是2的幂，设为2^m．这时$p_i=2^m+1$．如果$m=ab$，$a>1$而且a是奇数，那么多项式$x^{ab}+1=(x^b)^a+1$能被x^b+1整除，2^m+1这数可被2^b+1整除，因此2^m+1不是素数．所以m必定是2的幂．于是对于p_i就只是那些形如$2^{2^k}+1$的数的问题．对于$k=0, 1, 2, 3, 4$，得到素数3, 5, 17, 257, 65537．对于$k=5$，得到的数可被641整除，自此以后形如$2^{2^k}+1$的不必为素数．所以用规尺可作出的正n边形，正好就是那些n形如$n=2^\nu p_1\cdots p_r$，其中的p_i是形如$2^{2^k}+1$的不同素数．例如正17边形的作图读者可在文献中找到．

2．角的三等分．60°的角是可作的．这角的三等分得到18边形的作图，所以由例1是不可能的．

3．Deli的倍立方问题．（据传说）亚波罗要求把已有的立方形祭坛的体积加大一倍（仍然保留立方形状）．设原有祭坛一棱之长为1，则应作出$\xi=\sqrt[3]{2}$的图．于是$K=Q$，$F=Q(\sqrt[3]{2})$．因为x^3-2在Q中不可约，所以$(F/Q)=3$，因此要求的作图是不可能的．

译 后 记

作者 Emil Artin(1898～1962)的生平和数学贡献，可看 S. Lang 与 John T. Tate 1965 年合编的«The Collected Papers of Emil Artin»及其所附书目. 我只把这集子的合编者序的最末两段意译于下：

"Artin 生平爱好在各个年级教学. 即令身居研究教授之职，他定期开初等微积分的课，坚持不懈. 他的课堂讲义和讨论班讲演，以完美、精辟为世所称道，使得他的代数观点广泛流传. 荷兰数学家 van der Waerden 的名著«代数学»，就是整理、引申他和 Emmy Noether 二十年代末在汉堡和哥廷根的讲演；而在已往三十年来，一直是基本的参考文献.

"这些讲演和讲义，激励、启发了他的学生；他对他们的慷慨和爱护是无以复加的".

作者于 1958 年重返汉堡后，出版了此书的第三版(第一、二版(1941、1946)是用英文写的. 1958 年李英先生译出第二版，由上海科学技术出版社出版)，用德文写出，作了重要的改进(请参看作者序). 我把此书的英文第二版和本版仔细比较过，从第 II 部分 C 段起到最后，无论行文叙述、论证层次，都经作者精心整理重写；就是第 I 部分 E 段也有所更改. 这第三版是更为精辟、简洁了. 因为这些改进，以及此书已为作者名著之一，我们认为有翻译这第三版的价值.

聂灵沼先生对这中译本作了很多必要的修改. 至于德文口语难懂之处，钢铁学院赵锡霖先生指点实多. 由于江泽涵

先生不断地鼓励，这中译本才整理完成。我对三位先生深致谢忱。

译　者
1978年8月